

目录

1

战争与和平中的密码

我比较熟悉各种形式的秘密文字，也写过一篇关于这个问题的粗浅论文，其中分析了160种不同的密码。

歇洛克·福尔摩斯

（《跳舞小人》）

“大桥先生，如果我被判处死刑的话，我作鬼也会回来找你。”逃犯对秘密警察署的检察官说，经过多次审讯两人之间已经形成了一种和谐的气氛。1941年10月那个星期六清晨，当人们闯入记者R·佐尔格东京的家中，把穿着睡衣、趿着拖鞋的他带到警察署去时，大桥检察官也在场。

从那以后，犯人有足够的时间来思索他的生活。在牢房刚开始的几个星期中，这失败的新体验把他推入绝望。后来，一种起初较微弱之后逐渐增强的安慰感在他体内复苏，他的确成功地完成了任务，这种想法使他更能忍受不可知的未来

命运。在希特勒对苏联发起进攻之后，佐尔格向莫斯科第四局发出信息，日本不会从东边向苏联进攻。正是他的报告使得朱可夫元帅能够把军队、坦克和飞机从西伯利亚撤出来转移到莫斯科前方去对付德国人。难道不是他，R·佐尔格创造了世界历史吗？从审讯人的问话中他可以断定，日本人没能破译他加密的消息，他的报务员曾数千次地将这些消息发送到上海和海参崴的苏维埃电台。

报务员克劳森致电莫斯科

这个夏日，东京上空的空气令人窒息。马克斯·克劳森看着他前面桌上的纸条。过了一阵，文章才被破译。他读着——又是"奥托"发来的报告。上司从来没跟他说过，但是马克斯知道，"奥托"是小组中的一个日本同事，他的消息总是很重要。

1941年6月22日后，德国军队越来越深入苏联境内。很久以前，马克斯就向莫斯科发电警告，其中甚至还包括德国进攻的准确日期，然而那里却没人作出反应。也许，苏联在不久以后不仅要对付德国，而且同时——虽然在4月份已订立不进犯条约——也必须防御日本？日本在这几天里进行了战争动员，新组建的部队会被调往南方，还是调往北方，对付苏联？

"奥托"的报告弄清了一切。日本无论如何也不会进攻俄国，因为中国的事件已经够它忙的了，只要与美国的谈判结果尚不明确，没有一个日本人愿意与俄国打仗[①]。如果日本确

① F·W·迪金，G·R·斯托里：《R·佐尔格：一个著名的双重角色的故事》，慕尼黑，1965年，第259页。

实要进攻苏联的话，最早也应在明年，在这期间德国军队早已深入到俄国领土内部去了。看来希特勒在冬天来临之前想占领莫斯科。日本方面不会进攻的消息使苏联大大地松了一口气。报务员马克斯·克劳森开始了加密工作。

他虽然已熟知第一步，但这次还是用了一张纸，这张纸随后就会被销毁。第一步是将字母表中的字母与数字对应起来，为此他必须利用他的密钥词，即英语中“地铁”这个单词：SUBWAY。他按顺序写好这 6 个字母，然后在下面划了 4 条线，在这 4 条线中按顺序分别排入字母表中剩余的字母以及圆点和线符号(作为单词分开的标志)。这样，他就得到了图 1.1 上面这张表格。

因为他总是用英语发送信息，所以在这种语言中最经常出现的字母 a、s、i、n、t、o、e 和 r 对他来说就显得特别重要。“a sin to err”(犯错是一种罪过)这句话正是由这些字母组成的——这是一种帮助记忆的方法，对克劳森来说已没必要。这 8 个字母应分别分配给 0…7 这些数字，他将这数字填入表格，逐列逐列的，从左开始。一旦碰到“a、s、i、n、t、o、e、r 当中的一个字母，就按从 0 到 7 的顺序在下面写下其中一个数字。这样，他的表格就很像图 1.1 中间这一幅了。现在他在剩余的字母下按竖列顺序写下从 80 到 99 的数字，于是就得到图 1.1 下面这张表格。

现在，字母表中的每一个字母都有它对应的数字，利用它们，克劳森就能够将电文中的字母转换成一排数字。我们以一条简单的电文为例进行说明：按照德语“没有进攻”，即英语的“no attack”的顺序，产生了“729456658088”，这 12 个数字符号又可以被轻而易举地分解为与字母或字符相应的数字。如果字符前没有 8 或 9，字符将单个地与表格中的一个字母相

对应;如出现 8 或 9,则与下一个字符一起对应表格中的某个字母。在“729456658088”中,7、2、94 和 5 分别与字母(亦即符号)n,o,/和 a 对应,两个 6 对应双写是 t,80 是 c,88 代表字母 k。于是,“no attack”就被加了密,但这只不过是第一步,克劳森眼前得到的仅仅是暂时加密的电文而已。

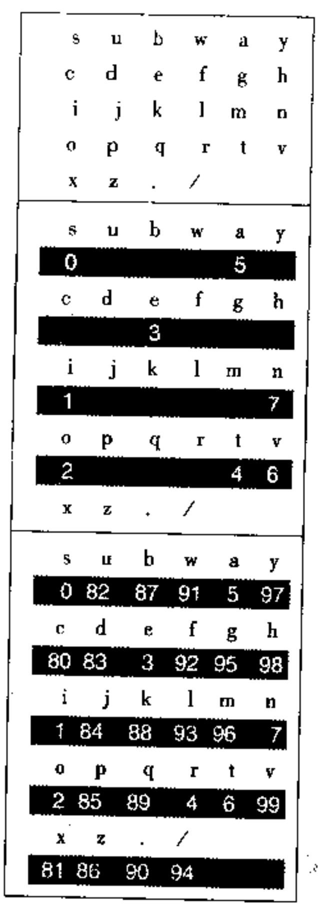


图 1.1:马克斯·克劳森用密钥词 SUBWAY 和 asintoer 这个提示词分三步制成一张密码表,利用这张表他可以将字母表中的字母转变成数字。

至此加密工作只完成了一小部分。每个新手都能发现，在用这种方式编写的长条消息中，数字“3”出现的频率最高，它与无论德语还是英语中都最常出现的字母 e 相符合。这样，每个窃码者都可以完成解码的第一步。所以，马克斯·克劳森现在才开始真正编写密码。他从书架上拿出 1935 年德意志统计年鉴，翻开充满数字的一页。他记下页码和表格中某个数字的行数和列数，他想从这个数字开始。这些是关于各个国家烟草生产的报告，其中有数字 4230，下面是 5166、7821、9421 等等。他必须从第一个数字的第三个数码开始，然后加入其他数字：30516678219421……这是莫斯科和他之间的一种老规定，而这一行数字才是真正的密钥。克劳森写下他暂时加密的电文，再在下面写上密钥：

729456658088
305166782194 . .

然后把它们相加，在这当中，如果和数超过 9，十位数就不进到前面一位，即不是 7 + 8 = 15 而是 7 + 8 = 5，计算过程见图 1.2 上，接下来他还得告诉接收人年鉴的页码以及行数和列数，以便对方可以从同一本书中查取密钥。就页码而言，两个数字就够了，因为如果给出 34，那么可以是 34、134 或 234，至于哪个是正确页码，接收人自己很容易就可以判断。就行数和列数来说，3 个数字也够了。236 指第 23 行第 6 列，所以 34236 总共 5 个数字就足够标识密钥的开头。克劳森将这 5 个数字放在他电文的开头，但把它们加密，方法是把密文开始的 5 个数字相加，同样再次排除十进位法，即将 34236 + 02451 = 36687。这样，他的电文就被分成若干组，每组 5 个数字：36687 02451 23301 72，然后向空中发送这些数字组。他知道，

接收人首先会把第一组数字减去第二组数字,不考虑十进位制:36687 - 02451 = 34236,这样他就获得了页码(34 或 134 或 234)以及行数和列数(23 和 6),即所有用来确定密钥的信息。现在他只需从接收到的电文中(排除用来找密钥的前 5 个数字)减去密钥;如图 1.2 下所示。

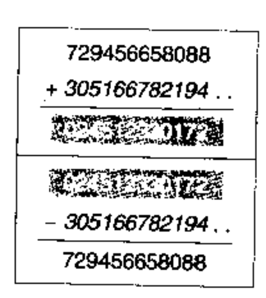


图 1.2 上:从一条数字化的,即已转变成数字符号的普通电文,通过密钥(斜体部分)变成一条数字化的秘密电文;下:从数字化的秘密电文到数字化的普通电文。

这样,他就得到了用这份表格加了密的电文,而且能轻而易举地将其译回普通电文,因为他手上也有图 1.1 下的那一份表格。

马克斯·克劳森每次都从不同的地方发送新信息。如果上一次是从自己的住所发送电波,那么下一次就从间谍组织中一位南斯拉夫同事的家里,偶尔在其他朋友那儿他也会架起电台,竖起天线。因此,虽然这些从东京向空中频繁传递的电波早已引起了日本秘密警察的注意,但他们却无法在这座人口密度极高的城市中测定和发现电台的方位。

为了不被测向车发现,在发报的过程当中克劳森也经常更换位置,他不时地将发报机从一个地方挪动到另一个地方,所以很有可能在这时撞上警察,但最后泄露间谍组织的却并

非电波,日本警察是在仔细调查日本共产党早期支持者的过程中,偶然发现的。

1941年10月14日晚,R·佐尔格想和他的日本同事尾崎秀实,这个专门提供消息的"奥托"碰头,但这人却没有在约好的时间露面,接下来的几天里也无法用电话与他联系上。克劳森在10月17日深夜即18日凌晨被捕,警署的人在大清早也敲响了佐尔格的门。对他以及他同事的审讯持续了3年多,尾崎和佐尔格于1944年10月7日被绞死;而克劳森被判终身监禁,他妻子也被处以服刑3年的惩罚。在日本投降以后,这两人都被盟军释放并逃往苏联,之后很长一段时间内再也没有听到有关他们的消息。

直到将近20年后的1964年10月,东柏林的一家报纸[①]刊登了一篇题为《马克斯·克劳森还活着》的报道,称莫斯科《消息报》的柏林通讯社在德国同志的帮助下,发现了克劳森夫妇,他们在民主德国首都过着简朴和隐居的生活,于是各种新闻媒体开始对此大肆宣扬。这对夫妇在一次疗养度假之后于1964年前往当时的苏占区,并化名为"克里斯蒂安森"定居下来,后来迁往柏林,东柏林报界将此二人誉为正直的共产党人和民主德国市民。直到此时民主德国的媒体才发现,马克斯·克劳森曾由于他"模范的建设意志"成为焦点人物,《新德意志报》从档案中发掘出一条已尘封9年的关于先进工作者"马克斯·克里斯蒂安森"的新闻,他那时是克珀尼克游艇厂的政治指导员,照片上的他正用尖头十字镐清除废墟。当时报纸还不知道这张照片上的人和谁有关呢。

据说当时他对自己的功绩秘而不宣,只是由于其谦逊的

---

① 1964年10月29日《新德意志报》。

性格所致。然而1964年沉默突然被打破，克劳森接受采访并详细谈论了他在日本与佐尔格从事的工作。克劳森——克里斯蒂安森突然又重新露面。关于先进工作者马克斯·克里斯蒂安森过去的报道显然直到1964年才被公开。因为每次就佐尔格周围间谍组织工作进行的深入的历史研究，都不可避免地涉及斯大林所犯的错误，即斯大林最后将佐尔格关于希特勒进攻苏联的警告当成了耳边风。但1964年已取消禁令，德国统一社会党中央委员会成员、民主德国国家广播委员会主席、老共产党员格哈特·艾斯勒可以光明正大地回忆他和佐尔格曾见过一面，老党员赫尔曼·西布勒也重新记起他和直到现在仍被人闭口不谈的R·佐尔格见面的情景。而格拉工具机器厂的劳动英雄埃伦弗里德·纳瓦拉则让他的生产小组在佐尔格生日之际举行一场劳动竞赛。81岁的马克斯·克劳森于1979年9月15日与世长辞，在此之前他早已被授予卡尔·马克思勋章、苏联红旗勋章以及其他高级荣誉称号。

日本人始终未能破译R·佐尔格忠诚的发报员发出的加密电文，因为编密方法早被精心设计了一番，而且关键是利用一本无关紧要的书，而这本统计年鉴可能在抄家时未被注意到。

小蜡板的秘密

发报员马克斯·克劳森致电莫斯科的方式令外行人无法读懂，而对于今天的编码人员来说却十分原始，他可以让电脑将一封发给一位澳大利亚同事的信加密，并通过网络寄出。但相对于初步尝试信息加密的人而言，克劳森已采用了一种相当不错的方法。

早在几千年以前，人们就已经开始交换秘密消息。世界历史上的许多事件周围都萦绕着有关秘密消息的传话，例如公元前480年著名的温泉关战役。

今天，在欧罗巴75大道上从塞萨洛尼基朝雅典驱车前行，经过奥林匹斯山后，便抵临拉米亚海湾，在那儿，高速公路沿海岸延伸。丘陵上的纪念碑使人回想起那场战役，在这次战役中斯巴达国王莱奥尼达斯抵抗由波斯国王薛西斯率领的优势兵力，但却徒劳无功。其实战争爆发之前莱奥尼达斯就在等待着波斯军队的到来，因为他已通过一封密信得知了这一消息。

正如希腊历史学家希罗多德所报道的一样，一个被流放波斯的希腊人送了一块小蜡板回国，一块与当时人们用于书写毫无二致的涂有蜡层的小木板。这人先除去蜡层，在木板上写下关于波斯人将大举入侵的消息，然后又重新抹上蜡并把它送给了莱奥尼达斯。由于这样一来这封信无法读出，于是得以畅通无阻地抵达希腊，不过如果不是莱奥尼达斯的妻子戈尔戈无意中发现了蜡层下面的字迹，这则消息肯定会被一直隐藏下去。莱奥尼达斯就是这样接到警报的。

然而，如同历史上屡见不鲜的事例一样，这封密信并没有对战争的结局产生什么决定性的影响。一个希腊的叛徒带着波斯人通过一条隐蔽的小路，越过山岭，偷袭莱奥尼达斯位于温泉关的驻地，于是莱奥尼达斯的军队被左右夹击，最后全军覆没。

根据希罗多德的记载，当时没人能从外面看出小蜡板里隐藏着至关重要的消息，估计蜡板上可能刻有一篇无关紧要的文章，使人根本无法注意那则真正的消息。

致桑道夫伯爵的密信

1867 年，的里雅斯特是奥地利帝国的一座城市，哈布斯堡王朝准备在它的北面建立王朝最大的港口，然而那年春天出现了种种不太利于该计划实施的迹象。几个月前，奥地利在克尼格雷茨战役中败给了普鲁士，而自从拉约什·科苏特领导的起义被奥地利人镇压下去之后，匈牙利的自由运动就从未平息过。

儒勒·凡尔纳的小说《马蒂亚斯·桑道夫》就是以这种紧张的气氛为背景的：匈牙利伯爵桑道夫暂时住在的里雅斯特，由信鸽给他捎去关于家乡独立斗争运动的加密消息。有一次，一封信件落入敌手，大意是人们已准备就绪，只等他一声令下便起义反抗奥地利，信文如下：

CAELHUREEENERDSSETAIISESTSNBIETZIEBIMHENUEN
WBIESENEVSRSTOIDNSCEEHNTNDERRENANLGLAIREE
NIFUGSNUXKEAXEBXHRIATDUE

奥地利间谍中当然无人能破译这封信，直到一个混蛋从伯爵的书桌里窃取密钥之后，他们才得以解开它。

密钥是一个由横竖 6 格组成的正方框。从 36 个正方格里剪去 9 格，于是形成一个编码板，如图 1.3 所示。接收人为解开密码，将秘密信文写成 3 个正方形，每个由 36 个字母组成，如图 1.4 上所示。现在他把编码板放在秘密信文字母组成的正方形上，通过剪掉的空格读出：allesistb（图 1.4 下左），然后沿顺时针方向将编码板旋转 90 度（图 1.4 下右），并读出：ereitbeim。再转 90 度：erstenzei，又一次转动编码板：chendassi。这样，第一个方

框的工作就完成了，与其他几个方框一起得出原文：

allesistbereitbeimerstenzeichendassieunsvontriestsendenwerdener hebensichallefuerdieunabhangigkeitungarnsxxx

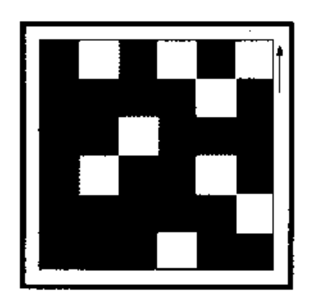


图 1.3：这是儒勒·凡尔纳在他的小说《马蒂亚斯·桑道夫》中所描绘的编码板，把它放在一张空白纸上，在框中剪去的（图中为白色）格里填入需要加密的消息的前 9 个字母，之后沿顺时针方向将编码板旋转 90 度，并在空格里填入接下来的 9 个字母。依此类推，直到编码板已转过 4 个方位为止，填入的字母在纸上构成一个长宽各为 6 格的正方形，按行读出，便得到了编好的信文。如消息更长，则又开始一个新的正方形；如方框不能填满，则任意选择字母补充信文，直到 36 个空格都被填满为止。











图 1.4：如何破译第 10 页上的加密信文。秘密信文被写成 3 个正方形，如上。将图 1.3 的编码板按照最初的形式放在第一个正方形上，如左下，右下为顺时针旋转 90 度后的情形，在这两种状态下，原文的前 18 个字母被重现出来。

为了让秘密信文填满3个正方形。信的结尾补充了3个增加的字母x。

玛丽亚·斯图亚特是如何被出卖的

大约在1586年，菲利普二世成为西班牙国王，他从父亲卡尔五世手中接过了一个世界王国，一个包括西班牙、西西里岛和意大利南部的王国，拥有哈布斯堡家族的所有财产以及西班牙遍及全球的殖民地。因此卡尔五世可以骄傲地宣称："在我的王国里太阳不会落下！"当1527年他的儿子菲利普出生时，即路德把他的论纲贴在维滕堡宫殿教堂的大门上之后的第十年，新教开始在欧洲各国传播开来。连苏黎世教士乌尔利希·茨温利也反对罗马教皇的教义。继而是瑞士法语区的J·加尔文，经他改革的教派传播到法国、荷兰、英格兰和苏格兰。菲利普二世让他奥地利的同父异母兄弟，唐·胡安管辖当时仍属于西班牙的荷兰，此人曾于1571年在勒班陀战役中与意大利人一道战胜了土耳其人，捍卫了天主教。被派往荷兰后，他仍把抵制福音新教的异端邪说，保护天主教教义当作自己在该处最重要的使命。

在英国，早在30年代，亨利八世就和罗马教皇闹翻了，这是因为罗马教皇拒绝宣布英格兰国王亨利八世与卡尔五世的姑妈卡塔琳娜结束婚姻的消息，也不赞成接下来他与一名宫廷妇女的亲事。在此之后，亨利宣布自己为英格兰教派的带头人，并强迫教士承认他的权威地位，以代替罗马教皇。于是在当时便形成了支持加尔文教义的英国圣公会。改革主要是在亨利的女儿伊丽莎白一世的统治下进行的，就这样，英格兰发展成为最强大的新教势力。

在苏格兰，加尔文教义也找到了支持者，在一次起义中，天主教女王玛丽亚·斯图亚特被驱逐出境，她在亲戚伊丽莎白的国家里寻求庇护，然而这两人之间的关系却异常紧张。国内的天主教徒认为，按照法律玛丽亚才是英格兰真正的女王，这招致她后来被伊丽莎白软禁了长达20年。

据说玛丽亚·斯图亚特是个魅力十足的女人，但这显然并不是唯一的原因，唐·胡安企图率领军队登上英格兰，迎娶玛丽亚，帮她坐上伊丽莎白的位子，与她共同治理这个国家。他还在信中告诉其他人他的这一想法，当然是以加密的形式，然而这种方式对他却毫无帮助，显然他没有考虑到英格兰的特务机构这一因素。

伊丽莎白一世在位时，英格兰国内的阴谋造反运动甚嚣尘上，以至于不得不建立秘密警察以维护国家制度。该机构的建立由伊丽莎白的大臣弗朗西斯·沃尔辛厄姆负责。当他几年前在意大利旅游时，就已强烈地感受到编写密码的重要性，而这在当地已有着悠久的历史。他创建了一个机构，单单在欧洲大陆上就安插了53个密探。这一举措的作用，不久就显露出来了。那时，荷兰一位深谙密码的贵族接到一封悄悄递来的密码信，一个月后他破译了该信。信是唐·胡安发出的，在信中他公开表露占领英格兰的梦想。沃尔辛厄姆的一个亲信在荷兰获悉该信内容后向大臣报告了此事。大臣认为，眼下正是十万火急的紧要关头，应对玛丽亚·斯图亚特严加看管。碰巧就在此时，他偶然收到一个名叫吉尔伯特·吉福德的囚犯的申请书，请求替他效劳。待此人刑满之后，沃尔辛厄姆接纳了他并委之以监视玛丽亚·斯图亚特周围动静的任务。于是，吉福德就作为信差混入了玛丽亚的人当中。

1586年，当玛丽亚在英格兰被软禁了20年之后，她的一

名支持者想出一条计划，暗杀伊丽莎白，引发英格兰天主教徒起义，从而让玛丽亚登上英格兰女王的宝座。吉福德奉令行事，从皇宫里偷出了玛丽亚及其侍从的所有信件，当然，他总是先将加密信件制成副本，然后再呈交沃尔辛厄姆。这位大臣有一位得力的密码专家，能帮他快速解码。据说玛丽亚在给这起谋杀策划者的一封信中祝愿他取得成功，这句话的破译便注定了玛丽亚的命运。沃尔辛厄姆首先抓了这些谋杀策反者，然后以谋反罪起诉这位苏格兰女王。这些在玛丽亚被捕时从她住处搜出大量密件的暗探，是否曾偷偷地放入伪造信件，就不得而知了。不过玛丽亚直到最后一刻仍一口咬定自己无罪。1586 年 2 月 8 日，她被送上断头台，刽子手砍了 3 次才把她的脑袋砍下。

铁面人之谜

或许这个面具根本不是铁制的，而是丝绒的，这个秘密究竟是否真的被揭开了，也尚无定论。故事概要：17 世纪 70 年代，萨伏依伯爵领地皮格内罗尔城的居民们注意到一个囚犯经常出现在监狱古堡的城垛之间，他的脸被一个黑色面具遮住。看守士兵说，这个囚犯享受极好的待遇，甚至还在古堡司令的餐桌上吃饭。人们传言说，这人有一次从墙上扔下一块刻有各种符号的小银板，城里的一个居民刚好路过，捡起这块板子，于是立即被警卫抓住，送进监狱。他在一间阴冷的小屋里被关了好几个星期，直到审问人相信，他既不会读书，也不会写字，更没有参与什么设法营救该囚犯的阴谋为止。后来这个戴面具的人被送往巴黎巴士底狱，被监禁长达 31 年后，于 1703 年死去。

这个神秘的囚犯激发了他同时代以及后来好几代人的想象力。亚历山大·大仲马,《三剑客》的作者,从他笔下还诞生了《基督山伯爵》,后来写了一本与之有关的长篇小说《铁面人》。谣言霎时传遍全国,铁面人是路易十四的孪生兄弟吗?又或是他的私生子?

1891年一位名叫维克多·让德龙的法国军官在研究历史时发现了一封密码信。由于这封信对他毫无用处,于是他把它转交给外交部密码处的艾蒂安·巴泽里斯。

巴泽里斯是一个法国军官,他尝试破译日报上(用密码加密编写的)人事通告,后来和密文打交道。那时,许多结了婚的人常和他们婚外的情人交换信息,他们刊登的消息如此亲密,以至于巴泽里斯的同伴们常常在食堂里以此为乐。巴泽里斯越来越多地练习阅读加密的文章。当他已44岁时,有一次他声称能轻而易举地阅读按照法国军事密码系统加密的消息。试验证明果真如此。于是国防部立即改换编码系统,但是不等新方法被采用,巴泽里斯已将它破译。他顿时名声大噪,被安排进外交部密码处就职。这时,他开始对几百年前的密文产生了兴趣,这些密文到目前为止尚无人能破译。他揭开了路易十四在位时一些文章的秘密,还能读懂拿破仑时期秘密来往的信件。于是维克多·让德龙把这封古老的密码信寄给了他。

1到500之间的数字在不规则的字行里交替出现,特别有几个数字经常出现。巴泽里斯猜测,每个数字代表法语的一个音节,但是单个字母也可能由一个或几个数字来表示。数字22出现得最频繁,有187次,然后是124,接下来是42、311和125,现在他开始把它们与一篇普通的法语文章中最常出现的音节对应起来。他假设,124可能是指冠词"les",22

1

5

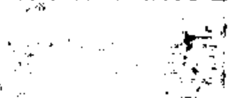
为"en",146 和 125 为"ne",并且作出结论,字母 s 可能由一串不同的数字来表示。至此,他成功地解开了几乎所有被加密的消息。这是一封由国防部长卢瓦写给皮德蒙特的军队司令、中将德卡蒂纳的信。

卢瓦在信中写道,布隆德将军由于拒绝执行命令应受到处分。国王命令,立即逮捕布隆德并将其押往皮格内罗尔城的古堡。晚上将犯人锁入一间小屋,白天则允许他带着 330 309 沿城垛走动。由于这两个数字在文中其他地方不再出现,所以巴泽里斯设法通过上下文猜出其意思。他听说过巴士底狱中面具人的故事,并且知道此人原来被监禁在皮格内罗尔,此外,他还得知这名犯人被当作重要人物来对待,因而他推断,数字 330 的意思应当是"masque",法语单词"面具",而 309 可能是某个句点符号。巴泽里斯宣布,戴面具的人就是布隆德将军。

伟大的巴泽里斯是否就此一语中的,仍然存在疑问。如果"面具",一个非军事用语,仅用一个数字就能将其加密,真有些令人惊讶。因为只为了代表常用词语,人们才从 500 个可能的密码数字中选取一个,而其他所有的单词则要通过数字逐个逐个字母地来表示。除此之外,据说布隆德在面具人死后还活了 5 年。

托马斯·杰斐逊的编码轮

想方设法破译秘密消息的都是些僧侣、军官、数学家和密探,但他们中间还有一位著名的政治家和国家元首托马斯·杰斐逊,美国独立宣言的起草人之一,美利坚合众国第三任总统。他发明了一台编码机,这台以他的名字命名的"杰斐逊



轮",在表 1 中可见。

它由 36 片同样大小的木片组成,它们的边被平均分成 26 段,边上带有打乱了顺序的字母表中的字母,每块木片上的字母排列都不尽相同:要找出 36 种不同的排列顺序,一点也不难,因为可以有很多种任意排列字母表中 26 个字母的方法。木片边上有从 1 到 36 的标记,中间钻孔的木片被放在一根金属轴上,也许 27 号木片在最左边,接着是 2 号,然后是 10、13 等等。发信人和收信人必须拥有同样的木片,并且必须将其在金属轴上的顺序排成一致。举个例子,如果发信人想传递秘密消息《angriffmorgenbeisonnenaufgang》(明早日出进攻),那么他就拿着带木片的金属轴与垂线成直角,将木片顺序调整好,使字母紧挨着连成一行,组成这则消息。然后固定木片,不让它们随意转动。现在如果他将这组木片绕轴旋转,就可以得到下面的 25 行字母,它们中的任何一行都是这则消息的密文,外人无法破译。比如,发信人选出一行字母,如下:

TOBQMVESBXUZKYGYMZAPXUWZAMRFT

他将这行字母寄给收信人,这人现在要将他的编码机调整到正好使这组字母排在一行内,接下来他只需在其他 25 行字母中找出有意义的那一行来就行了,如果他的木片也和发信人的一样排列,那么他就会找到《angriffmorgenbeisonnenaufgang》。

编写密码的技术在欧洲已有悠久的历史,而杰斐逊似乎是单枪匹马地发明出了他的编码器。即使窃码者拿到了这 36 块同样大小的木片,如果他不知道它们的排列顺序,实际上也无法解开加密的消息。杰斐逊已经知道,木片顺序的排列方法是[illegible]数。这台杰斐逊轮被证明效果显著,所以第二次世界大战时美国海军仍在利用它。

墓碑和墙上的符号

8　在离纽约华尔街股市不远的地方,有一座有着200多年历史的古老教堂,三位一体教堂,在幢幢摩天大厦之间显得渺小而破旧。它是上几个世纪留下的产物,被纽约商业区的高科技和交通噪音包围着。在旁边的公墓里,游人可以找到詹姆斯·利桑的墓碑,他死于1794年9月28日。利桑曾是共济会成员,“耶路撒冷共济会第四分会”会员。碑石上的墓志铭旁的上方有一行符号,如图1.5所示,只有掌握密钥的人才能读懂这些秘密符号,每个符号代表字母表中的一个字母,这些字母的排列极简单,可见图1.5下。碑文为:remember death(记住死亡)。

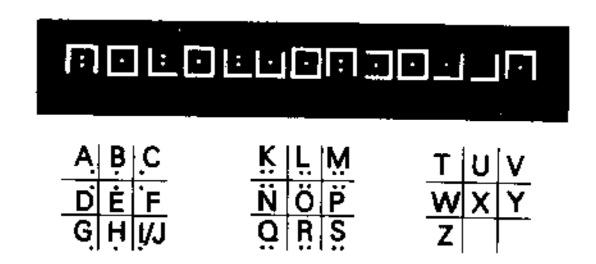


图1.5 上:詹姆斯·利桑坟墓上的密码碑文。下:字母表中的25个字母被分成3组,每个符号中的圆点数标明附属的字母可在哪一组中找到。符号部分的边缘则决定框中的字母。这些符号十分简单,所以很容易用锤子和凿子在石碑上敲出。

我们不久将会看出,这种加密方式很容易被破译。共济会成员可能并不是为了通过加密使这些文字保密,而是希望在碑文中体现他们这个组织的神秘性。

但美国共济会也没有编写好他们真正的秘密,而其他兄弟会在这方面做得也并不比他们更好。美国内战不久后成立

的“美国联盟团”(OAU)也有着同样的秘密规定。谁想参加它的活动,必须说两遍暗语。成员之间常用密码转告这些经常更换的口令(图 1.6),他们不能交出密钥(图 1.7)。我们将看到,这又是一次简单的加密,即使不知道密钥也能轻易地将它解开。在这种情况下,编密的动机与其说是为了满足保密的需要,不如说是使秘密行动产生吸引力。

图 1.6:美国国内战争(1861—1865)后美国联盟团的秘密口令。

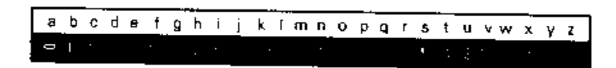


图 1.7:破译图 1.6 中密文所需的密码字母表。

不仅有着崇高目标的社团利用密码,而且三 K 党也有它的密码,近 3 个世纪以来的小偷和杀人纵火者也在围墙和房子的墙壁上使用秘密符号,以便给他之后打这儿路过的同伴以指点。图 1.8 所示为其中几种符号及其意义。



图 1.8:小偷的暗号,1915 年左右发现于格拉茨,意思为:黎明上路,前往人民公园(树)附近有轨电车车站旁的十字路口。四声鸟叫。寻找支持。丰厚的赃物,注意(冒号),28 号在人民公园旁的公共厕所里碰头(根据汉斯·格罗斯和弗里德里希·吉尔茨,《犯罪侦察学手册》,第一卷,柏林 1977 年,第 92 页)。

加密的技巧

人们把改变一篇文章，使之无法让外人阅读的技巧称为"加密"。"密码学"是一门关于加密和脱密的学科。我们将看到，即使采用乍一眼望上去十分保险的加密方法，一条被加密的信息，也能够被破译出来。

克劳森致电莫斯科的例子已能解释几个基本概念，这几个概念将在此书中贯穿始终。需要传达的信息称为"明文"，如我们例子中的"没有进攻"。报务员克劳森分两步将其转化为一行数字，这是"密文"，以克劳森的电报文为例，即 34236024512330172。在詹姆斯·利桑碑文的例子中，明文为箴言"记住死亡"，密文为图 1.5 上面那行符号。在这本书中，所有的明文(尽可能的)用小写字母，所有的密文用黑底白字或白色大写字母来表示。

克劳森在莫斯科的收信人能开始他的脱密工作，是因为他掌握了"密钥"，也就是说，因为他知道，该采取什么办法将密文重新转变为明文。在 OAU 的秘密文字中，密钥如图 1.7 所示。利桑的共济会分会为其所做碑文的密钥为图 1.3 中的方框。密钥应严格保密，因为任何人都可以通过它将密文转化成明文。在此书中，密钥(尽可能地)用斜体大写字母表示，如果密钥为一行数字，则数字也用斜体来表示，即：

Klartext , *SCHLÜSSEL* , GEHEIMTEXT

在这一章中你已认识了两种完全不同的加密方法，发报员克劳森将数字经过复杂的换算之后替代明文的字母，杰斐逊用其他字母来代替原来的字母，即使在明文中不出现 x 或 y，也可以将 a、b、c 换成 F、X、Y，这种用其他符号代替明文符

号的编密方法称为 Substitution(置换),该书中几乎所有章节都涉及到置换法。相反,在桑德尔多夫伯爵的秘密文字中仍保留了明文的字母,只不过它们出现在密文的其他位置上。如果明文中没有 x 和 y,那么它们在密文中也不会出现。如明文中包含 5 个字母 f,那在密文中也可找到 5 个 f。这种编密方法称为 Transposition(移位),第 8 节中将谈到。

无论是置换还是移位,在传递信息之前,发信人和收信人必须对密钥取得一致。第一次世界大战当中军舰上备有许多厚厚的类似百科全书的密码本,在这些书中,每一个明文单词都对应了一长串的密文符号。将明文转化为密文,就如同利用字典将文章逐字翻译成外语一样。第一次世界大战刚开始时,俄军得到德国海军的一本信号书(第三章),因此能够轻松地破译德方海军的电报。

一方面发送尽可能更多更快的加密信息,另一方面为了能够快速破译敌方电报,加密和脱密工作不再限于手工操作。为了能在较短的时间内阅读第二次世界大战中用德国编码机“恩尼格玛”(第九和第十章)加密的电报,英国的科学家和技术人员研制出了第一批电子计算器,作为解码机使用。第二次世界大战后计算机被应用于密码破译法的实践。

随后,科学家不仅制造出更好的机器,能够更快地加密和在短时间内脱密,而且还发明了一种不再需要交换密钥的方法,成为密码学历史上的里程碑。以前,每个想发送加密信息的人都必须冒着被窃码者得知的风险,想方设法传递密钥。今天发信人无须预先将密钥交给对方,就可在任何公开场合发送只有真正的接收人才能读懂的密文。

近几个世纪以来,日益精密的加密方法被研制出来,但同时挖空心思、违法地对付密文的方法也逐渐增多。读者将会

详细地了解到密码学迄今为止最新的发展情况，然而首先还是让我们来研究一下秘密信息最简单的传递方式吧。克劳森的电报由一行行无直接意义的数字组成，桑道夫伯爵的密文是连在一起的字母排列，而共济会会员的密文是一串符号。所有看到这些秘密信息的人，肯定都会猜到，这是加密信息，莱奥尼达斯收到的小蜡板则不同，它可以通过边境检查，因为没人会想到里面还藏着秘密信件，这种加密方法根本不会让窃码者一开始就猜到里面带有秘密信息，对此我将在下一章中详细谈论。

2

从隐藏的信息到密本

所谓的斯特哥图解在计算机中发展到了极点。程序员罗玛娜·玛查多同时也是一位非常成功的人体模特，编制了一个名叫斯特哥的破坏性程序，可任意将数据藏到电子图像后，……它是如此令人难以捉摸，以至于观看者完全摸不着头脑，教皇的肖像是否实际上是炸弹制造说明。

《明镜周刊》1996/36，第 211 页

一个刑事犯想稍微改变一下他的生活环境，却不能写信叫妻子在他的生日蛋糕里藏一包炸药，因为即使监狱长官执行任务时再如何宽宏大量，当他看到这封信时，也会觉得这个生日愿望不合适。这个犯人也不能将自己的心愿用密码的形式表达出来，因为一封带有一行似乎毫无意义的符号的信同样通不过检查——相反，长官自己更会先试着去破译信的内容。这个可怜的犯人只有一条路可走，即寄一封看似无关紧

要的信回家，这信不会令人生疑，但却隐含着只有他的妻子才能发现的秘密愿望，因为她知道怎样去寻找隐藏的信息。怎样将秘密信息藏在一封人皆可读的信里而不会引起怀疑呢？

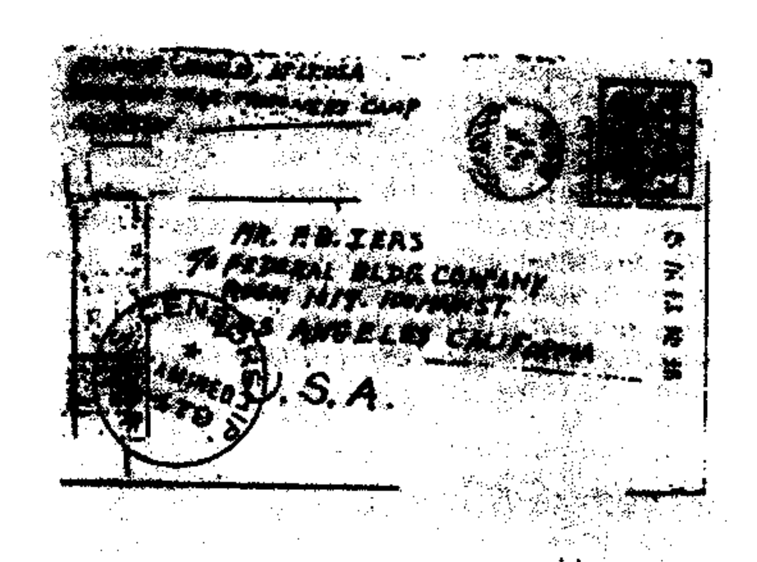
普通信件中的重要消息

1943年秋，战争仍在进行，一天，一位邮差站在洛杉矶中心大道100号大楼前，按照地址，明信片应投到1619室一家联邦建筑公司，有一位F·B·伊厄斯先生在这儿工作。然而这幢楼里既无这家公司也无1619室。最后，这张明信片落在了619室，联邦调查局，简称FBI，在此设立了一个办公室，收信人名字的首字母和公司的名称显示出明信片（图2.1）应寄往该处。它寄自日本的一所战俘集中营，并通过了日本和美国的检查，发信人是一个名叫弗兰克·G·乔纳里斯的少尉。FBI的人估计，这封信一定有什么特殊之处，果然——当他们将每一行的前两个字读出，便得到下面这句话："After surrender fifty percent Americans lost in Philippines in Nippon 30%."[①] 这是关于美方损失的消息，被藏在一张普普通通的明信片里。

早在16世纪时，意大利的医生和数学家杰罗尼莫·卡尔达诺——我们以后还会讲到他——就曾思考过，怎样将消息藏入一封在普通读者看起来无关紧要的信中，他建议采用一个类似于桑道夫伯爵所使用的编码框。这个方框只将信中的某些字母显示出来，从这些字母中就可读出密文。当然，发信人和收信人都必须拥有同样的编码框，这个编码框就是密钥。

---

① 《密码学》，1980年4月，第120页。将这则被隐藏的消息译成德语为：投降后，美国人在菲律宾损失了50%，在日本30%。



DEAR IERS:

AFTER SURRENDER, HEALTH IMPROVED
FIFTY PERCENT. BETTER FOOD ETC.
AMERICANS LOST CONFIDENCE
IN PHILIPPINES. AM COMFORTABLE
IN NIPPON. MOTHER: INVEST
30%, SALARY, IN BUSINESS. LOVE



图 2.1:一张第二次世界大战中从日本战俘集中营寄给洛杉矶联邦调查局的明信片畅通无阻地通过了日本的检查机关。将每一行的前两个字连起来读,就可得到关于美军损失的消息。

Lieber Wolfgang

übermorgen früh schickt Herr [illegible]
Mitarbeiter, Herrn Fritz Bauer, z[illegible]
er mit Dir noch einmal über[illegible]
len Vereinbarungen spricht[illegible]
voll vertrauen. Herr Frey [illegible]
Brief noch heute per Boten[illegible]
weil Du Dich auch noch vo[illegible]
dafür die früheren Belege p[illegible]
mußt.

Bis nächste Woche! Dein

Emil

图 2.2:在一封普通信件中藏着一条十分重要的消息,只有将一个仅能读出单个字母(图中为白色)的编码框(图中为灰色)放置其上时,消息才会显示出来。

并不一定非得采用编码框。赫伯特·W·弗兰克在他名为《秘密消息》[①] 的书中为了说明另一种方法,举了一则电报为例:"Noch einmal tiefempfundene Anteilnahme. Rasche Rückkehr erforderlich. Von Norbert alles Liebe. Paula."(再次致以深切的哀悼。速归。诺伯特祝一切顺利。保拉。)如果从后往前读出每个单词的首字母,就可以得到一条秘密信息。(译者注:消息为"计划泄露")小蜡板(第 21 页)则是另一种例子。这种传递信息的方式,令窃码者猜想不到其中还藏着秘密信息,称为斯特哥图解。同属于此的还有一种方法,突出某些字母却让外

① 《法兰克福汇报》,1982 年,第 28 页。

行人无法认出。

1996 年 5 月，毛皮加工师傅卢茨·赖因施特罗姆被判终生监禁。原因是他把两名妇女关在一间小屋里，折磨她们并最后将其杀死。为了干得不露痕迹，他强迫受害者给他们的亲属写贺卡，主要是让他们知道，这二人已跑去国外了。这些卡片后来由他寄出。其中一个女人在信中附加了一个求救信号，并且指出该虐待者的姓名，她采取的方法是将某些字母写得较粗些——白费心机，隐藏的信息被忽视了。赖因施特罗姆把女人的尸体装入啤酒桶里，用酸溶解。突出的字母直到后来才被一位专家发现并用来审判凶手。图 2.3 显示这起汉堡酸桶杀人案受害者所写的带求救信号的两张卡片中节选的部分。



图 2.3：汉堡酸桶杀人案受害者之一隐藏的求救信号。在上段中通过加粗的字母隐藏着“hilf”（帮助）这个单词，而这个女人在下段中则通过加粗的字母“luz”暗指凶手的名为“Lutz”（卢茨）。

1976 年出版了一本关于推理的书[1]，两位数学家海因茨·里夏德·哈尔德和维尔纳·海泽在书中描写了一道古老的数学难题，所谓的柯尼斯堡的七桥问题。如果仔细阅读此文，稍动

① 《推理入门》，慕尼黑，1976 年，第 118 页。

脑筋就可发现,有个别字母印得更粗并稍稍往下移动了一些位置,将它们读出便可得出这句话:“打倒苏维埃帝国主义”。

隐藏的信息中还包括用隐显墨水写在信的边上或字里行间的消息。这是一种无色液体,通过加温或某种化学处理又能显现,经验十足的特工在无色墨水用光之后,以尿代之,效果也不错。

战争期间,德国反间谍机构想出一个办法,将信息拍摄下来并缩小,直到可以将它整个放人一张微型底片中,然后将这张底片藏在打字机打出的信的句末点号下。

有些隐藏在看似平常的信中的消息,不仅窃码者,而且有可能连收信人自己也会忽略,这是一件十分自然的事情。约翰·特里文爵士很可能得到过某种暗示,否则不会发现救他性命的秘密暗示。约翰爵士是英国一个忠贞的保王党人,落入奥利弗·克伦威尔之手并被监禁在科尔切斯特城堡内。他的两位朋友已经在那里被处决,他也面临着被处死的命运。这时,他接到一封信,落款人为 R·T,直到今天历史学家仍未弄清这位发信人的身份。我从这封用古代英语写成的信中摘录开头和结尾如下:

Worthie Sir John: - Hope, that is ye beste comfort of ye afflicted, cannot much, I fear me, help you now. That I would say to you, is this only: if ever I may...

...have done. The general goes back on Wednesday. Restinge your servant to command. - R.T.

虽然这个故事被人们反复讲述,但我却从未找到解释,约翰爵士是从何处看出信文中隐藏着秘密消息,而且是由每个标点符号后的第三个字母组成的。通过这种方法可以从全文

中得出这句话:"panelateastendofchapelslides"(小教堂最东边的墙板可以移动)。约翰爵士从信中找出这条信息后,请求看管人允许他在小教堂里忏悔一小时——然后就逃走了。

不过也有可能出现错认为一封普通信件中藏有秘密消息的情况。

莎士比亚是如何撮合一桩婚事的

第二次世界大战中被美国人称为"紫密"(见原书249页)的日本编码机的解密方法与一个人名紧密相关。此人是世界上最著名的密码学家之一,或许也是有史以来最伟大的密码学家。

1891年,威廉·F·弗里德曼生于俄国,第二年随父母移居美国。他顺利地念完了高中,毕业时,属于300个学生中最优秀的前10名。弗里德曼首先在一家推销蒸汽机的公司里任职,后来还上了一所农业学校,最后在纽约州伊萨卡的康奈尔大学学习植物栽培。为了供自己上学,他在一家餐馆当招待。正在这时,一个富有的纺织品商乔治·费边,想为他的农场找一个懂植物栽培的人,希望通过他的帮助来提高收成。他向康奈尔大学询问合适的人选,并于1915年聘用了弗里德曼。

费边未受过任何科学教育,但却拥有自己的实验室,工作人员在实验室内研究声学、化学、遗传学以及密码学。弗里德曼虽然被安排在遗传学实验室工作,但由于他会摆弄照相机,所以也帮助密码学家将旧的文章放大。一共有十几个人专门研究伊丽莎白一世时期的信件,费边主要是想找到证据,证明莎士比亚的作品其实是由伊丽莎白手下的弗朗西斯·培根爵士所写。150多年来,这种想法一直在文献中作祟。美国政治家伊格内修斯·T·唐利曾认真地刨根究底:他想弄清

是否能在莎士比亚作品中找到"Bacon"(培根)这个词,如果没公开出现在明文中,也许可能以某种密码的形式出现。于是,支持这一说法的人纷纷展开调查,是否在莎士比亚的作品里出现了可以理解为名字"Bacon"密码的词语。

培根的确曾对密码感兴趣,甚至发明了一套自己的解密系统。调查有何结果?在莎士比亚的作品中能找到暗示培根的地方吗?人们在剧本《空爱一场》第四幕第三场中找到下面几行字:

> ...But with the motion of all elements
> Courses as swift as thought in every power,
> And gives to every power a double power.

从每一行的第一个字母和第二、三行的第二个字母可以得出:

> B
> CO
> AN

这就是弗朗西斯爵士姓名中的字母。然而,如所有其他证据一样,这一发现也未被当作令人信服的证据。一个爱开玩笑的人提出莎士比亚写了第46首诗,以此嘲讽那些"培根化名莎士比亚假说"的信徒们。事实上,在这首诗的英文翻译中,从头算起第46个单词是"shake"(摇晃,晃动),如从后算起会发现第46个单词为"spear"(矛,枪)。然而自学成才的费边没有被此迷惑,他竭尽全力证明,培根用"莎士比亚"这个名字作为笔名。伊丽莎白·史密斯,一个银行家和政治家的小女儿,也从1916年起开始从事该方面的研究。不久,弗里德曼

和她紧密合作，他们倾心于密码学，而且也倾心于对方。1917年5月，两人结为伉俪。就这样，“培根化名莎士比亚假说”使他们两人走到一起，虽然他们很早以前就已经知道，在莎士比亚的作品中，根本没有隐藏什么暗指其他作者的地方。后来他们写了一本关于这个问题的书。

当美国加入第一次世界大战时，弗里德曼已升任费边密码部的负责人，从这时起，除研究莎士比亚作品外，他还从事其他重要工作。不久后，这个研究部名声大振，连政府机构都请求他们的帮助。例如，交给他们从印度寄往柏林的密文，一部分印度人希望在德国的帮助下实现国家的独立。弗里德曼破译了这条密码和其他的加密信息。后来，他给军官上了密码学方面的课，他的课在该学科内开辟了一条全新的道路。他用一种维吉尼亚加密方法成功地确定了密钥字的字数，当卡尔斯基方法行不通时，可求助于它。[①]

鲜为人知的是，1924年他被请求破译火星人的密码。这一年，火星距离地球特别近，是有史以来最近的一次。突然间，许多美国海军的无线电台宣称收到了陌生信号，但是弗里德曼却从这些信号中看不出什么意思，这可能是由于无线电干扰的缘故。

1940年8月弗里德曼开始进攻日本的“紫密”，经过20个月艰苦的工作后，他能展示最初被破译的“紫密”无线电讯号。

防空洞里的掷骰子游戏

1941年12月7日，日本未发出警告便偷袭美国驻夏威夷

① 这些概念将在第六章中解释。

岛上的珍珠港海军部队。一个月以后，美国联邦调查局间谍罗伯特·L·希弗斯从檀香山提醒华盛顿的联邦调查局局长J·埃德加·胡佛注意，11月22日这期《纽约人》杂志第86页上曾刊登了一则广告，替一种掷骰子游戏大作宣传(见图2.4左)。





图2.4：第二次世界大战中1941年在《纽约人》上刊登的一则广告。在1941年12月7日日本偷袭珍珠港之后，这家公司被怀疑曾利用此前刊登的宣传掷骰子游戏的广告暗示了这一日期。难道间谍可以通过右边图画中的骰子提前得知袭击的时间吗?

这幅图的上部分画的是荒凉的野外，炮弹爆炸和探照灯照亮的夜空，下部分是一群人在防空洞里似乎兴致勃勃地玩着掷骰子的游戏。下面写着一句话“注意！警惕！警报！”。然后是一段话，指出，人们除了罐头、蜡烛、水瓶、毛衣、被子和

书本以及维他命药片之外，还应带上"致命的加倍"这种掷骰子游戏，花 2.50 美元就可在所有的大体育用品商店和百货商店买到。另外还有多则小广告暗示了这则大型广告(见图2.4右)。在这些广告上面分别有两个骰子，如果将两个 X 看作是死亡的象征，第一个骰子看作月份，第二个骰子看作日期的话，那么，图中就暗示了 12 月 5 日或 12 月 7 日这两个日期。骰子上的数字是一条秘密消息吗？12 月 7 日开始袭击珍珠港，难道日本已经散布了这则消息，以提前两个星期向在美的日本人宣布军事行动的开始？

希弗斯的报道第一个指出了这家王朝印刷公司的广告问题，随后一系列怀疑接踵而来；美国联邦调查局在当时不得不对此展开调查。在调查为什么在美国人毫无准备的情况下袭击珍珠港这一问题的过程中，这家王朝印刷公司理所当然也被彻底地仔细了解了一番。公司属于某一位克雷格先生，这人在调查时显得非常合作。调查人员没有找到什么可以对其采取法律行动的证据。他在一封也许写给一位新闻记者或电台记者的信中申明自己无罪，而《纽约人》的出版商则认为这是对无辜百姓的迫害和诽谤。

在调查过程中还出现了许多问题，而克雷格先生也无法再对此作出回答，因为他在 1946 年就去世了。据说他来自马萨诸塞州的波士顿，但却没法打听到有关他过去的情况，而他也从未出具过他的出生证明。

或许这些骰子只是在无意间公开了这个灾难性的日期，因为情况证明，早在一年前他们就曾为同样的掷骰子游戏做过广告，广告上骰子摆法也一模一样。没有人真的会认为，1940 年就能准确地预言偷袭珍珠港的日期。

1979 年，大约 40 年之后，英国达特默思大学一位学生在

为他关于第二次世界大战的博士论文查找资料时，也碰到这例旧广告，同样，他也注意到其中暗藏着袭击珍珠港的日期。①

账号中隐藏的信息

人们在一段文字里加入其他信息，并不总是为了传递某些秘密的东西，密码常常用来防止书写或转抄错误，例如，我们的每个账号中都含有一个纠错码，它多半可以用来验证这是否是指银行的账户。

我们举一个德意志银行账户为例，号码为0291864，现在，我们想检验它是否是德意志银行的账户。先去掉最后一个数字，剩下的就是“原来的”账号029186，现在我们开始从右算起，6在第一位，8在第二位，1在第三位，然后9在第四位，2在第五位，0在第六位。接下来找出所有单数位置(从右算起)上的数字并且将它们翻倍:4、2、12。如果结果是两位数，像这里的12，那就用两位数字之和代替这个数，12的数字之和为$1+2=3$:

0 2 9 1 8 6
  4   2   3

然后将双数位置上的数字照原样写在下面:

0 2 9 1 8 6
0 4 9 2 8 3

① L·克鲁:《致命的翻番广告》，密码学，1979年7月，第170页。

把它们相加:0+4+9+2+8+3=26。我们现在加上原来账号中省去的最后一个数,如果这的确是一个德意志银行的账号,那就必须得出一个完整的10的倍数。在我们这个例子中的确是一个真正的账号,因为26+4是30。倘若我们不用它而用0291865作为账号,那我们验证的结果则不是一个完整的10的倍数,这就表明该账户不是德意志银行的。所以账号的末尾数字是所谓的"检验数字",可以用来检验填写数字时是否出现错误。也就是人们所说的银行账号被"加密"。如将两个相邻的数字换位,如8和1,计算结果就不能得出整数,账号也不一定就是真的。如果将2错写成3也完全一样,但即使检验正确,这个账号也不一定就是真的。我们有可能不是将两个相邻的数字倒换,而是将中间隔着另一个数的两个数字换位,即将8和9换位,这样,检验的结果不会因为数字的改变而变化。账号中的密码虽然在多数情况下能起作用,但却不能绝对防止错误的出现。

我在此选取了一个德意志银行的账户作为例子。其他货币机构有其他的加密方法,即其他的计算法则,以避免可能出现的书写错误。顺便提一句:您的信用卡也被加了密。

信用卡中的检验数字

我们以一张号码为0699004313139642的Visa信用卡为例,从右边开始算每个数字,2是第一个数,0是第16个数,现在在下面写出所有单数位置上的数字,即:

0699 0043 1313 9642

6 9 0 3 3 3 6 2

然后将双数位置上的数字加倍，同时在原来的数字下写出结果。如加倍时得到一个比 9 大的数，则减去 9，于是得出：

0699 0043 1313 9642
0699 0083 2323 9682

再把下一行的数字相加：

0+6+9+9+0+0+8+3+2+3+2+3+9+6+8+2。信用卡号码计算的结果也必须能被 10 整除。我们得出的总数为 70，正合适。反之则不然：如得出一个能被 10 整除的数，不一定说明原来的数字就是一个信用卡的账号。

我在这儿仅以 Visa 信用卡为例，其他的信用卡也有一个检验数字，根据这条或那条规则与卡号相配。

每本书都是独一无二的

……即使作者从头至尾都是从其他地方抄袭来的。ISBN 的代码保证了它的唯一性——这是世界标准书号代码的缩略，世界标准书号代码是一个十位数，可以用来清楚地标识每一本新近出版的书，只要将你要订购的书 ISBN 号码交给书商，如果有货的话，他肯定能够帮你订好。刚才你读的那本书的 ISBN 号码为：

3 498 03495 2

它由 4 组数构成。第一组数表示该书出版的国家，3 代表德语区。英语国家如美国、英国和加拿大为 0，2 代表法国，7 代表中国。接下来的一组数字是出版社的代号。罗沃尔特出版

社的代号是 498 和 499,492 是慕尼黑的皮珀尔出版社,421 是斯图加特的德国出版社。该书第三组数字才代表出版社的内部统计数。这样,这本书就被清楚地标识出来。我们知道了国家、出版社和标明该书的号码。第四组数字由 0 到 9 中的某个数字或者罗马数字 10,即 X,组成,这是一个检验数字,通过它可以看出前面的数字中是否出现错误,以至于使你在订购时得到的不是约瑟菲妮·穆岑贝歇尔的回忆录,而是马克斯·普朗克学会的年鉴。如果 ISBN 代码正确的话,下面的计算方法必须成立:把第一个数乘以 10,第二个数乘以 9,第三个数乘以 8 并以此类推,直到把倒数第二个数乘以 2 为止。把结果相加,直到最后一个数,最终的结果必须能被 11 整除。如果不是这种情况,那肯定是有什么地方不对。

我们以代码 342102765X 为例。如你所知,末位上的 X 代表 10,在 ISBN 号码中你能看出,此书是在德语区(首数为 3)里的德国出版社(第二组数为 421)出版的。代码对吗?你在每个数字下按递减的顺序写出 1 到 10。

3 4 2 1 0 2 7 6 5 X
10 9 8 7 6 5 4 3 2 1

分别将上下两个数字相乘,上行中的 X 则看作 10。

$3\times10+4\times9+2\times8+1\times7+0\times6+2\times5+7\times4+6\times3+5\times2+10\times1=$
$30+36+16+7+10+28+18+10+10=$
165

这个数能被 11 整除!所以你可以肯定,利用这个代码将会获得我的朋友彼得·梅茨格尔关于《寒冷的宇宙》一书。

3　如果你在书写时出现错误，如将第3位上的2写成3，那么计算的结果就不能被11整除，你的书商的聪明的电脑即刻就能发现这一点。同样，如果你将两个数字交换，如将第三组数

8　02765写成02675，他也会指出来。你可以核实一下，检验数字是ISBN代码中的隐藏信息，通过它能够发现转抄中的错误。

从隐语到密本

让我们回到隐藏在普通文字中的重要信息上来，这些信息无法让外人读懂。最原始的方式是用别的东西代替某些词语或句子。所以军队喜欢将他们的行动冠以无关紧要的名称。希特勒对苏联的进攻是**巴巴罗沙**行动。盟军占领西西里岛的代号为**赫斯基兰特**。**霸王**是指盟军的诺曼底登陆，而**女武神**这一代号是指1944年7月20日那次旨在干掉希特勒的失败尝试。

第一次世界大战期间，一位英国检查官发现两名商人每天通过电报进行大宗的雪茄交易，这些雪茄来自英格兰的港口城市。进一步调查后，他们暴露出自己是德国间谍。如果一个人订购5000支纽卡斯尔的科罗纳雪茄，意味着在那个港口停靠着5艘巡洋舰。海克·扬森和威廉·罗斯因此被抓并于1915年7月在伦敦的监狱里被处死。

1944年，**霸王**军事行动，即进攻诺曼底前不久，法国的反抗者们准备为法国的解放作出自己的贡献。为了通知他们即将发生的登陆行动，英国无线电台在法语节目中向空中发射法国诗人保罗·魏尔兰诗篇的开头部分：LES SANGLOTS LONGS DES VIOLONS DE L'AUTOMNE（大意：秋天小提琴的啜泣），即这是对即将到来的进攻的暗示。接下来对时间作

了更为详细的预告：BLESSENT MON COEUR D'UNE LANGUEUR MONOTONE(使我的心持续悲痛)——标志着进攻将在 24 小时之内开始。

替换词语的系统越精密，就越有必要开列出长串的词条作为《词典》。如词汇书中，左边是明文中的概念，右边是与之相应的密文，一个字母或数字的组合或者两者兼而有之。16 世纪西班牙的菲利普二世交给他的官员的《词汇手册》——这是那些罗列单词的清单的名称——包括大约 400 个密码词语。在新大陆上，乔治·华盛顿的间谍使用的词汇手册约有 800 个词条。

用于加密的密本第一次被大量运用是在美国独立战争期间。1780 年 7 月 15 日，即英国将军查尔斯·康沃利斯率领英国军队在弗吉尼亚的约克敦投降的前一年，本尼迪克特·阿诺德寄了一则密码信息给约翰·安德烈，一个年轻的英国秘密警局军官。阿诺德是西点军事基地的指挥官，据说后来在那里建立了美国军校。他在一本当时很有名的法律评论中逐个寻找他的明文词语，然后确定页码、行数以及词语在行中所在的位置。如果其中有一个单词他在这本书中无法找到，那么他就以字母的方式将其加密，也是通过给出这个以找到的字母开头的词的页码、行数和位置的办法，并且用下划线标明他所指的只是这个单词的第一个字母。这就使加密相当复杂。设想一下，你必须用 1964 年菲舍尔出版社出版的托马斯·曼的《约瑟夫和他的兄弟们》作为密本，并想编写"ich habe gestern raumschiff enterprise gesehen"这句话(我昨天看见宇宙飞船厂)。"ich"(我)在 274 页，38 行，作为第一个单词就编成 274.38.1；接下来"habe"(助动词)是 172.19.4，"raumschiff"(宇宙飞船)必须用字母的方式改写；r 是 10.1.13，a 写成 8.

1.5,u写成9.1.6,m为9.9.3等等。“enterprise”(企业)这个词托马斯·曼那里可能没有出现,所以你又面临着另外10个字母,然后你必须找“gesehen”(看见)。从这个例子已能明显地看出这是种多么费时的大胆行为。

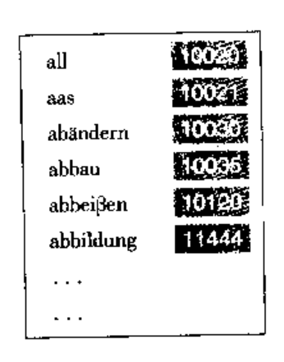
不久后,阿诺德转向一本字典,他能在字典里按字母顺序的编排中更快地查找单词,但却仍然不能避免用字母的方式给罕见的单词加密。在给安德烈的加密信件中,阿诺德向英国将军亨利·克林顿要价2万英镑,以提供能占领西点和其他驻地的信息,并在英国人进攻时投降。这笔交易最后泡汤了,因为这个英国秘密警察局的人被美国军队抓获。人们在他的住处发现了有关西点的资料并把他当作英国间谍绞死。美国人阿诺德得知这一消息后,潜逃到英国。

1785年,托马斯·杰斐逊总统和将成为他接班人的詹姆斯·麦迪逊共同设计出一种密码,在这种密码中,数字组合被分配给单个词语。1370与单词peace(和平)相对,paper(纸)是207,Paris(巴黎)是1042,但在此期间杰斐逊却一直用明文写信,只把某些单词替换成数字密码。

不久,这些长长的清单便被编成了“密本”。自1630年起,人们可以分辨出好的和坏的密本。直到那时,明文和密文的词语都分别按词典编写方法排列,假设密文由5个数字构成,开始部分可能看上去如图2.5所示。这种编排的优点在于,能够利用同一密本进行加密和脱密。像在词典中一样,借助于字母排列顺序可以毫不费劲地找到每个明文词语,但又能够通过数字找到每个密文单词,因为这5个数字即使不是一字不漏地逐一编号,也是按照数值大小进行排列的。然而,这种方法的缺点也显而易见:如果一个窃码者已证实11444是“abbildung”,那么他就能肯定20451的明码文在单词表中

肯定不会出现在"abbildung"之前,所以无论如何不可能是"abbeißen"。直到路易十四在位时他的密码学家安托万·罗西尼奥尔才开始采用所谓的"二分式密码"。但为此他需要两本密本,一本是按词典编写法排列的明文词语的词条,另一本是密文词语的词条,这种书类似于我们现在由两部分组成的字典:法德/德法和明文—密文/密文—明文。缺点当然是必须用两本书工作。

密本在商业领域内也有其用武之地。谁要想让一封电报的费用维持在尽可能低的水平上,就应避免将某些词语如:"abfindungsanspruch"(结算权)、"gesellschaftsvermögen"(公司财产)或者"auseinandersetzungsguthaben"(资产清算余额)全文发出。有人提了个好建议,给自己编一本密本。如果在这本密本中不仅把单个词语,而且还把完整的习惯用语收录进来,例如:"Wenn Sie nicht binnen dreißig Tagen"(如果您不在30天之内)或者"mit freundlichen grüßen"(致以亲切的问候)。那么会更省钱。这种密本的目的不在于让外人无法读懂,而只是用来节约电报费用。不过这只是迈向密本的一小步而已。



all	10020
aas	10021
abändern	10030
abbau	10035
abbeißen	10120
abbildung	11444
...	
...	

图 2.5:一体式的词汇手册表

奇怪的是，德国海军还在第一次世界大战中采用了一种一体式的密码。图 3.1 所示为其中的节选部分。谁发现 53435 是“bōig”(起大风的)就已经能确定，62250 的明文在单词表中肯定出现在离 b 很远的后头，实际上它的意思是“märz”(三月)。

罗马教皇的密本

文艺复兴时期，教皇周围聚集着世界上最优秀的密码学家，例如阿尔真蒂一家，他们采用便于记忆的提示词方法。[①] 当时的罗马是一个世界权力中心，而有权力的地方，就有阴谋诡计和内部纠纷，于是破译对手的信息便成了当务之急。随着教皇权力在全世界范围内的衰退，其密码学家的水平也逐渐下降。但 19 世纪在梵蒂冈仍有一个黑屋。3 位密码学家(*cifristi*)在其中负责加密，受一名秘书领导。当时，教廷与最重要国家的教皇使节之间的信息还一直以加密的形式进行传递。然而只有少数秘密需要转告，因为常常已过了好几个月，罗马教廷与教皇在西班牙的使节之间才交换了唯一的一则秘密消息，而且实际上，这些信件中很少有什么特别重要的内容，于是也不值得将其加密。因而，在这种工作气候中加密的技巧不得不萎缩。

那时还有人建议，按顺序数出消息中的句子数，并在每个奇数句子中写出明文陈述的相反意思。每个罗马教皇使节都研制出了他们自己的加密系统。荷兰海牙的教皇使节用 MUSEUM(博物馆)代替“vatikan”(梵蒂冈)，用 MR.CERNI

---

① 报务员 R·佐尔格以“subway”和“asintoer”作为提示词。(比较第 13 页)

(塞尔尼先生)代替"Össterreich"(奥地利)。维也纳的教皇使节利用3个或4个数的数字组合发明了一本词汇手册。专有名词通过以7开头的4位数来表示。7690这组数字的意思是"拿破仑·波拿巴",有趣的是数字5在其中扮演的角色,它没有任何意思而且可以到处乱插,目的在于为难那些窃码者。[①]

罗马教皇的密码学家就是在20世纪中也未做得更好。里斯本的教皇使节在第一次世界大战前曾使用过的两本密本能让人了解教皇的秘密文字。[②] 一本用于编密,另一本用于脱密,其中也是明文和作为密文的数字组互相对应。密文符号是739个从000到999之间的3位数,但不包括7,因为这个数字像前一个例子中的5一样,有着特殊作用。每个3位数对应一个字母(643 = t),一个数字(005 = 13),或者一行意大利语常用字母(833 = zione),但也可以表示一个完整的单词(655 = italia)。图2.6是里斯本教皇的密本的节选。其中单复数没有区别,数字组毫无间隔地依次排列。脱密者无需理睬数字7,先将密文分成3位数的数字组,然后在用于脱密的密码书中寻找这些3位数的明文。这是一种并不十分精练的方法。

在第一次世界大战中,对立方利用密本主要是为了使军事以及外交信息保密,德国人遭遇了历史上的两次重大失败。

① A·阿尔瓦雷斯,"19世纪早期的教皇密码部门",《密码学》,1993年4月,第219页。

② A·阿尔瓦雷斯,"教皇的外交密码",《密码学》,1992年4月,第174页。

[illegible]	ra-e	[illegible]	democratico
948	congresso	984	dispo
949	ottanta	985	en
950	sospen	[illegible]	es
[illegible]	subito	[illegible]	graziz-e
[illegible]	quindici	989	ebbero
[illegible]	quattro	990	nerisi
954	ud	991	piu
955	f	992	o
956	n	993	at
958	ro	994	ar
959	nove	995	c
960	po	996	risolu
961	fra	998	va-e-u
962	proclam	999	ur
963	opportuno	7700	Damao
964	culto-i	7701	S.Tommaso
965	cinquanta	7702	Coccino
966	ogni	7703	imperatore
968	ad	7704	pacifico
969	alla-e	7705	Faro
980	an	7706	Austria
981	avano	7708	marchese
982	canonica-o	7709	concilio

图 2.6:二分式密本的节选,1910 年前后,教廷用它与里斯本的教皇使节交换信息。

3

第一次世界大战中的密本

无线电台海军中士诺伊豪斯最后拿到了电码本。有人看见他在水里，但似乎没拿那本书……当无线电台海军二级下士基勒尔特身在甲板之外时，他把电台的信号密钥用力紧握在手中。他是被跟踪的人推到水下面去的，当他再次浮出水面时，密钥已不知去向。

马蒂·E·梅科勒《马格德堡的秘密》

1915年7月的波罗的海，第一次世界大战爆发后的第一年，无线电通讯异常活跃，但是德国军舰的发报员不能译出所有电码，因为俄国人也坐在莫尔斯键旁发送加密信息。德国人无法确切地知道谁在发报，消息又是发给谁的，他们对向空中发送的命令内容一无所知。俄国人的情况则不同，他们能够破译德国人的电报，他们知道每艘军舰所在的位置及其途中所负的使命。所以，俄国司令员、海军少将巴契列夫可以有

目标地调遣他的部队,例如干掉德军布雷舰"阿尔巴特罗斯"。俄国海军的这种优势应归功于一年前同样发生在波罗的海上的一件事情。

"马格德堡"搁浅

1914年8月25日。这个月的第一天,德国向俄国宣战。海军少将贝林站在芬兰湾的入口,旁边是两艘巡洋舰"奥格斯堡"和"马格德堡",以及两艘护航的鱼雷艇。他想在那儿用鱼雷向俄国的装甲巡洋舰发起攻势并在返回的途中截获敌方的鱼雷艇。17点时两条船的方位都已测定,双方地理坐标之间相差一海里,然而却无人注意到这一点。海军少将站在旗舰"奥格斯堡"的甲板上,"马格德堡"跟随其后相距约1000米左右,这是为了万一"奥格斯堡"触雷,"马格德堡"还能有机会离开危险区。当时水手在雾中根本无法辨认其他船只。德军估计附近有一个俄军的水雷封锁区,于是在23点零3分,"奥格斯堡"通过电报通知"马格德堡",从现在起应向东南航行。这发生在23点零7分。目前双方正以每小时15海里的速度在新航线上航行。军官和岗哨都站在"马格德堡"的指挥台上,周围浓雾弥漫。俄国人肯定在附近的某个地方。"马格德堡"正朝奥登斯霍尔姆岛航行。只要能确定已绕过雷区,它就必须重新转向南,离开小岛,驶进芬兰湾,朝圣彼得堡方向前进。甲板上的人不知道,比起原来测定的方位,他们实际上更靠近奥登斯霍尔姆岛约一海里。"马格德堡"上的船员此刻也未被告知旗舰早已转向南航行。人们至今仍未弄清楚为何直到零点27分"奥格斯堡"才发出命令,重新改变航线,4分钟之后电

报被破译，舰长哈贝尼希特于是下令"向左 15 度！"，太晚了，船反应得太慢，当零点 38 分他们感觉到第一次猛烈撞击时，船仍在转向，随后紧接着好几次碰撞，最后，船迅速停了下来，所有没站稳的人都被摔到了甲板上。"马格德堡"搁浅了，水涌了进来。右舷水深只有 2.5 米，而左侧的测深锤显示水深为 5 米。

所有希望通过减轻重量开动军舰的尝试都失败了。即使把锚和链条抛到甲板外，将洗涤和饮用水池倒空，也无济于事。弹药和一切松动的多余铁制零件都被扔进海里，船却依然纹丝不动。接下来舱门被除去，但蒸汽机车以最大的马力倒车，仍无法移动这艘船。

破晓时分，船员们可以看见波罗的海海底的石头，他们发现，船搁浅在距离奥登斯霍尔姆岛仅 300 米的地方。哈贝尼希特舰长下令朝电台发射 120 枚榴弹，以免俄军获悉"马格德堡"的危难境地。太晚了——奥登斯霍尔姆岛上的岗哨已向俄军侦察部队长官、海军少校尼贝宁报告，在雾中听到有人讲德语，所以可能在奥登斯霍尔姆岛前方有一艘德国船搁浅。

在第三次试图开动军舰之后，"马格德堡"舰长决定放弃。现在必须销毁秘密物件，皇家海军 1913 年 1 月 7 日的电码本上写着这条指示："如电码本面临落入敌手的危险，必须将它抛入大海或（用火）销毁。"由于海水较浅，所以只能将这秘密文件烧掉。而此时，俄军频繁的无线电联络让人估计到，敌方军队不久将出现在海平面上。紧张的销毁行动开始了，锅炉房里，海军把书本和文件扔进火中，"马格德堡"上有 3 份这种电码，而其中的 2 份在慌乱中被忽视了。此外，地图室里还留着几张有关德军在波罗的海水雷

封锁区的海图。

一部分船员被护航的德军鱼雷艇救走。不久后，当俄军中尉登上该船时，甲板上还剩下的6名船员投降。舰长也还呆在舰长室里，他被俘虏了。接下来的几个月中，“马格德堡”的残骸被彻底检查，所有保留下来的文件都被收集起来进行研究。为了不引起怀疑，他们散布谣言，说“马格德堡”上载有大量的黄金和钱财，需要长时间地打捞。后来，俄军潜水员在海底发现两份灌了铅的电码本。

在指挥官哈贝尼希特放弃“马格德堡”后的第十一天，俄国驻伦敦海军专员向海军大臣温斯顿·丘吉尔报告，俄军手中已掌握《皇家海军电码本》(SKM)并已破译个别德军电报。他向丘吉尔提出所有文件可供英国人使用，这位英国海军大臣为此激动不已。10月份，两名俄国军官已将两份电码本中的其中一份以及其他材料送往伦敦。

“40号房间”里“马格德堡”军舰上的电码本

俄国军官带到英国的是一本密本，图3.1所示为其中一页。丘吉尔将它转交给一个研究小组，这个小组自开战以来就一直在从事密码研究。

第一次世界大战爆发的第一天，一个名叫“特尔科尼亚”的英军电缆工出海剪断了德国在埃姆登前方的海外电缆。现在，几乎被敌人全部包围的德国只能利用经过敌方领地的国际电缆，或者通过无线电与外界联系，因此所有消息都必须加密。鉴于这种情况，英国人决定创建一个密码破译小组。英国海军少将亨利·F·奥利弗即刻就物色到一个能创办这种机构的合适人选。

Zahlen- Buchstaben- Signal		Bedeutung
534 27	C a E	Bodenanstrich
28	C a F	Bodenbeplattung
29	C a G	Bodenbeschaffenheit
534 30	C a H	Bodenbeschlag
31	C a İ	Bodenstück
32	C a J	Bodenventil (Nr. n)
33	C a K	Bodenverschluß +
34	C a L	Bodenzünder
35	C a M	Bö ·ig
36	C a N	Bogen
37	C a O	bogenförmig
38	C a Ō	Bogenlampe
39	C a P	Bohle
534 40	C a Q	Bohne (n kg)
41	C a R	bohren ·ung, Bohr· *[s. Grund]*
42	C a S	Bohrer
43	C a T	Boje, Bojen· *[s. Anker, Kohlen, Leine]*
44	C a U	Boje auf den Anker stecken
45	C a Ū	Boje aufnehmen (fischen)
46	C a V	Boje auslegen
47	C a W	Boje beleuchten
48	C a X	Boje über Bord
49	C a Y	eine Boje über Bord werfen und wieder fischen
534 50	C a Z	an der Boje festmachen
51	C a γ	an die Boje gehen
52	C γ A	Boje falsch hinlegen
53	C γ Ä	Boje legen

图 3.1:"马格德堡"军舰上密本的节选。奇怪的是居然采用一体式的密本,其缺点第 40 页文中已作说明。

今天，每个物理专业的学生在基础课上都会认识到磁性物质有一种特殊性质，1880年左右一个英国人和一个德国人同时发现了这一点。这名英国发现者詹姆斯·艾尔弗雷德·攸英为此创造了一个新名词“磁滞现象”，今天人们仍在使用这一名称。攸英在东京大学工作了5年并在那里建立了一个地震观测站。回到英国后，他在剑桥执教，由于学术上的功绩被封为贵族。

第一次世界大战爆发前不久，攸英开始对密码学产生兴趣。于是海军少校奥利弗想到，把这位59岁的英国人争取过来在海军情报所里创办一个密码小组。攸英接受了这项建议并开始着手研究所有能弄到手的贸易密本，其中也包括德国的。但他的进展很缓慢，而这时从收音机里接收到的德国加密信息却越来越多。攸英为他的项目争取到许多同事，主要是海军学校的教师，他得知他们会德语。现在，这本“马格德堡”军舰上的密本也摆在了他的面前，虽然有这本书的帮助，这些德国电文仍不能马上破译。这时，其中一个人发现一些密码已被二次加密，采用的方法很简单，如后来所证实的一样，但攸英周围的这群人仍然花了将近三个星期时间才克服这道难关。不过后来他们就能读懂德国海军的电报了。

当更多的同事加入到攸英的小组中来时，1914年11月，他们搬入古老的海军部大楼第40号房间。从现在起该小组名为“40号房间”，这个小组迅速壮大起来，当1917年著名的“齐默尔曼电报”(见54页)被破译时，“40号房间”里已有800个报务员和将近80个密码学家以及办公室职员。40号房间对于他们来说早就变得太狭小，但当他们找到一个更为宽敞的处所时，这个名字还是被一直沿用下去。

"40号房间"里荟萃了各路精英人物。小组中包括一位古典考古学教授和许多高校外语教师,特别是德语教师,有个同事后来成为牧师并因翻译《圣经》而出了名。其中有个人是著名影星埃莱奥诺拉·杜丝的女婿。小组中还有一位同事,律师的儿子威廉·F·克拉克,他父亲曾在对奥斯卡·王尔德的审判中为其辩护,几十年后,克拉克成为第二次世界大战中布雷契莱庄园(见208页)里最著名的解码家之一。另外还有一位著名的时装设计师。秘书只能由海军军官的女儿或姐妹担任。她们至少必须掌握两门外语,据说照料她们的那个女人还会抽烟呢。

"马格德堡"的密码并不是"40号房间"里的人获得的唯一一份来自德国的材料。早在8月初,一群英国人就从一艘德国商船上缴获一本《德国贸易交往书》(HVB),这艘船上的船员对战争的爆发还一无所知。1914年11月30日,一艘英国渔船打捞到一个装满书籍和文件的铁箱,它是在一艘德国驱逐舰沉没之前,被它根据规定扔进大海的。"40号房间"的工作人员很快就觉察到,铁箱中不同的密本和这本《交往书》(VK)不仅可以用于战舰间的无线电通讯,而且还能用于柏林和德国驻外使馆海军专员间的信息交流。

怎样使美国不加入战争?

第一次世界大战中的第三个冬天。德国和它的同盟者1914年参战时的激情早已冷却,双方都已付出了惨重的血的代价。1916年夏,德军在凡尔登损失了28万多名士兵,他们或死或伤或被俘虏,在战役中损失的人数就达22万。法国方

面损失31.7万人,英国为27万人。没有一个作战国家占领了敌人的重要领地。英国本是中欧列国[1]最危险的敌人,由于他的岛国位置而变得安全起来。触及这个国家敏感处的可能性只有一种:切断这座岛屿的所有国外货物来源。只有当美国和加拿大的小麦运输船只以及载有瑞典钢材的商船再也不能靠近这座岛时,英国才有可能被战胜。于是在同盟国中就产生了利用潜水艇把所有朝这个岛国航行的船只击沉的计划,对中立国的船只也不例外,但主要是针对美国,在这次战争中已是第二次制定这项计划。于是,美国就不得不被一次打击商船的潜水艇行动扯入战争。中欧列国已经有足够多的敌人,罗马尼亚不久前也刚向它们宣战。

然而,德国人却认为能够对付美国加入协约国的举动。自从墨西哥不得不将它以前管辖的得克萨斯割让给美国后,这两个国家之间的关系就开始紧张起来。双方对对方领土的干涉使这种敌视气氛继续升温,于是德国的战略家认为,如果美国和墨西哥之间爆发战争,将会把美国人拴在他们的大陆上,从而防止其插手欧洲战争。这样就能使德国在这场潜水艇战中获胜。除此之外,日本也有可能在美国与墨西哥发生矛盾时派出部队在加利福尼亚海岸登陆。当时,墨西哥和日本正保持着一种友好往来关系,这令美国人忧心忡忡。

美国政府顾问罗伯特·蓝辛认识到这一危险并在他的备忘录中发出警告:“德国希望我们和墨西哥之间发动一场战争,正因为如此我们才不能这样做。”但也有人投反对票。《芝加哥论坛》写道:“命运在于墨西哥为我们准备了一个金苹果,

---

① 中欧列国包括:德国、奥匈帝国,自1914年11月起的奥斯曼帝国以及自1915年10月起的保加利亚。

而在佛兰德只是苦涩的果子。我们如果向墨西哥开战，那么就会知道，将获得什么——一个安全的大陆。实际上，我们不可能会输。"[①]

在德国，关于潜水艇战的问题仍然存在争议。帝国首相特奥巴尔德·冯·贝特曼·霍尔维格持反对意见。但是总参谋部中的"鹰派成员"，兴登堡和鲁登道夫都极力赞成此项计划，自1916年起他们就有统领德国的最高指挥权。决定是在上西里西亚南部波兰边境上的普勒斯堡（今普茨茨拉）作出的，德国总司令部在此设有驻地。最后，蓝眼睛的将军们得出结论：美国的加入没有战略意义。他们认为，德国只需半年潜水艇战就肯定会胜利，而到那时，美国恐怕还根本没有让其战争机器完全运转起来。兴登堡和鲁登道夫说服了当时仍犹豫不决的德国皇帝。贝特曼·霍尔维格提出警告并摘引德国驻华盛顿大使约翰·海因里希·伯恩斯托夫伯爵以及其他美国专家的报告，这些人严重警告应阻止美国参战。然而这位首相却得不到支持，因为毕竟还有墨西哥这张王牌。普勒斯堡垒的人们最后决定于1917年2月1日发动无限制潜水艇战。战区的所有船只，无论是敌方的还是中立国的，不发出预先警告就将受到鱼雷袭击。贝特曼·霍尔维格评论道："Finis Germaniae"——这是德国的末日。他本想辞去职务，然而这势必会造成军心涣散，于是他只好打消这个念头，尽他的职责，前往柏林，违背自己的意愿，以获取德意志帝国议会的批准。从副总理卡尔·黑尔费里希口中流传出一句话："现在德国已输掉了几百年。"

这就是这封加密电报产生的政治背景，它会创造历史。

---

① 巴巴拉·W·图赫曼：《齐默尔曼电报》，纽约，1958年，第90和95页。

齐默尔曼电报

在这次引起灾难的普勒斯堡会议召开前6个星期，国务秘书阿图尔·齐默尔曼当选为德国外交部国务秘书——这是第一次由一个平民获取该职位。然而不久就有人在背后议论他，说他比皇帝本人还高傲，而且更糟糕的是，他有极富冒险性的想象力。他认为，如果进行潜水艇战，一个墨西哥—日本同盟将花去美国人的全部精力，因此他们会避免卷入一场欧洲战争，德国驻墨西哥大使费利克斯·冯·埃克哈特报告说他的东道国与日本之间显示出一种友好的关系。军官们认为，如果墨西哥和日本分两条战线与美国同时作战，墨西哥将能够收复失去的得克萨斯地区。

齐默尔曼给埃克哈特发了一封电报，内容如下：

"我们计划在2月1日进行全面的潜水艇战争。我们将尽力使美国保持中立，如不成功，则建议墨西哥在下列基础上与之结盟：共同作战，共同缔结和约，我方完全支持并同意墨西哥收复以前失去的领土得克萨斯、新墨西哥和亚利桑那。

详细规定阁下来制定。一旦决定与美国开战，有劳阁下在严格保密的情况下向总统透露上述想法，另外，倡议日本立即自愿参战并同时在我们与日本之间进行斡旋。请向总统指明，我们现在毫无顾忌地运用潜水艇将迫使英国在短短几个月内求和，请确认收函，齐默尔曼。"

齐默尔曼起初打算将这封信随商业潜水艇"德国"送往墨西哥，这条船本应在1月15日出发，然而此次航行却被取消。现在这条消息不得不通过电报传递给埃克哈特。美国人自己将这个机会送到了他的手中。

在墨西哥,没有一个广播电台有足够灵敏的接收机,可以收听柏林附近的瑙恩电台发出的信号,但是美国设在长岛上的电台"谈笑风生"却拥有该技术条件。那时,美国总统伍德罗·威尔逊那时一再试图让欧洲战争的双方和解,而作战方对他提出的和平建议却充耳不闻。在他努力促成双方通过谈判达成一致意见的过程中,他允许德国驻华盛顿大使伯恩斯托夫伯爵通过美国电缆以加密的形式与柏林政府联络,这一举措使威尔逊在政界中遭到猛烈抨击,因为如此一来,德国人也可趁机交换间谍机构间的信息,但这位总统却执意坚持自己的决定。

齐默尔曼总共可通过三条途径将电报发给伯恩斯托夫,然后由他转送给墨西哥的埃克哈特:第一条途径是通过无线电广播从瑙恩发往"谈笑风生",第二条途径可由美国驻柏林大使馆递送这份电报,它与自己的政府间有电缆连接,或许也曾在不知晓内容的情况下发送过密电。最后,他还可以让人将电报带到瑞典驻柏林的使馆,瑞典虽为中立国,但同样会允许通过他们的电缆将加密信息发往美国。

为了确保安全,齐默尔曼决定,同时采用这 3 种方法,而无论是瑞典的还是美国的电缆都经过英国,于是电文也就 3 次落入"40 号房间"的人手中。

电报被破译

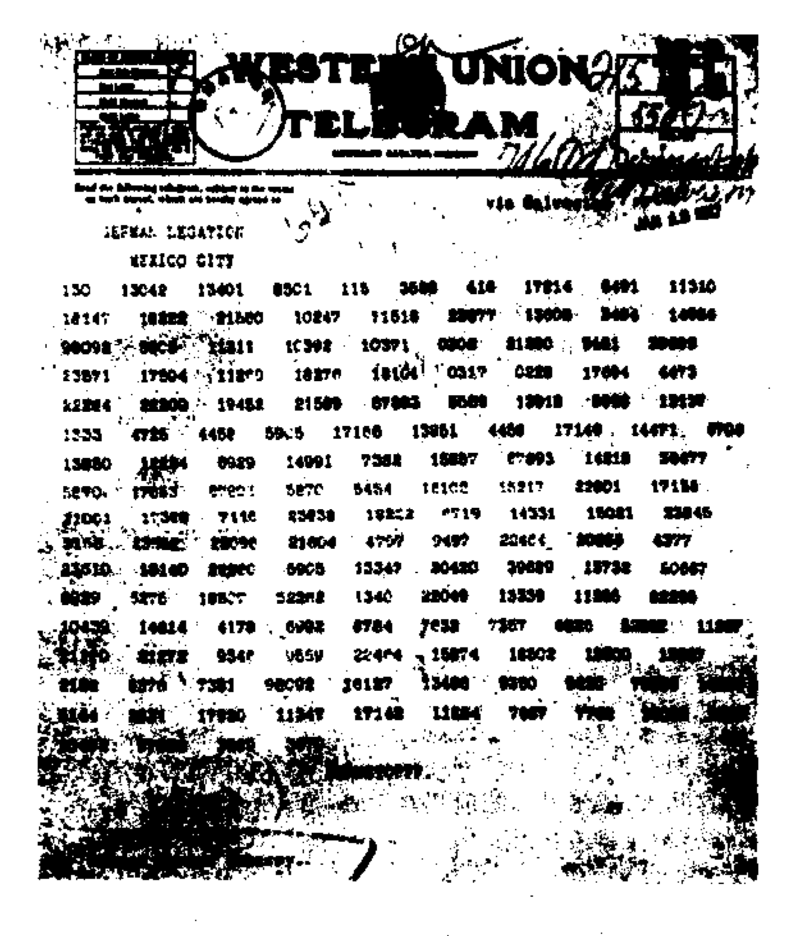
1917 年 1 月 17 日早晨,一个管道输送容器落入"40 号房间"的接收篮中,里面有一张纸条,纸条上是分别由 3 位、4 位和 5 位数组成的数字组(图 3.2),威廉·蒙哥马利和年轻的奈

杰尔·德格雷[1]仔细阅读起这张纸条来。第二组数字是13042,这让人想起外交机构通常在电报开头使用的密码,它标识所用的密本,但"40号房间"的人对代码13042一无所知,不过在他们的保险箱里有一本密本13040和一本列举该密码各种不同用法的书,这些用法是在苦心钻研上百条加密电文之后总结出来的。在电报末尾倒数第二位上的数字为97556,一般大的数字只用于姓名或罕见的概念。因此,末尾这组数97556显然是签名,实际上在密本上这个数代表名字"齐默尔曼"。这封密电是由德国外交部国务秘书亲自发出的,但它是发给谁的呢?蒙哥马利和德格雷突然发现17214,它表示"严格保密",接着注意到23845,意思是"阁下",——密本13040用于必须使用礼貌格式的书信往来。因为这个消息是在发往华盛顿的途中截获的,所以"阁下"所指的只能是德国大使伯恩斯托夫伯爵。另外,借助保险箱中的密本,他们还破译出其他一些词:67893是"墨西哥"。这个词在电文中甚至出现了两次,一封从柏林发给德国驻华盛顿大使的德国电报和墨西哥有何相干呢?他们接下来又发现"同盟"(12137)和"日本"(52262),这两个词同样也出现了两次,现在可以将单词逐个排列,于是前几行句子就断断续续地显露出来。

"我们计划在2月1日进行无限制潜水艇战。我们将尽力使美国保持中立,……不……,则建议墨西哥在下列基础上与之结盟……作战……缔结和约……墨西哥……阁下……与美国开战……严格保密的情况下向总统透露……日本……同时在我们与日本之间进行斡旋,……请向总统指明,……潜水艇……使英国在短短几个月内求和。请确认收函。齐默尔曼。"

---

① 德格雷在第二次世界大战中也是布雷契莱庄园的"恩尼格玛"解密者之一。



WESTERN UNION TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310

18147 18222 21560 10247 11518 23677 13605 3494 14936

98092 5905 11311 10392 10371 0302 21290 5161 39695

23571 17504 11269 18276 18101 0317 0228 17694 4473

22284 22200 19452 21589 67893 5569 13918 8958 12137

1333 4725 4458 5905 17166 13851 4458 17149 14471 6706

13850 12224 6929 14991 7382 15857 67893 14218 36477

5870 17553 67893 5870 5454 16102 15217 22801 17138

21001 17388 7446 23638 18222 6719 14331 15021 23845

3156 23552 22096 21604 4797 9497 22464 20855 4377

23610 18140 22260 5905 13347 20420 39689 13732 20667

6929 5275 18507 52262 1340 22049 13339 11265 22295

10439 14814 4178 6992 8784 7632 7357 6926 52262 11267

21100 21272 9346 9559 22464 15874 18502 18500 15857

2188 5376 7381 98092 16127 13486 9350 9220 [illegible] [illegible]

5144 2831 17920 11347 17142 11264 7667 7762 [illegible] [illegible]

[illegible]

图 3.2:齐默尔曼电报,与伯恩斯托夫发给墨西哥的埃克哈特的电报样。

通常情况下,德国人会对利用密本编写的密电进行第二次加密,但是在这封电报中他们却省去了这一环节。因而从这些支离破碎的句子中已经能看出大概意思。信的内容是如此令人惊诧,连破译者都几乎不敢相信自己的眼睛。直到那时,威尔逊总统仍在犹豫,是否应对处于困境中的协约国提供

帮助，而现在他们居然将这项卑鄙的计划摆到了桌面上——从墨西哥和日本两方面同时向美国施加压力——这不得不使他改变主意。

与完整的电报相比，“缔结和约”(17149)与“阁下”(23845)之间的句子当时除了“墨西哥”这个单词之外都未能破译，而在这部分正好是齐默尔曼许诺将促使美国在战败后得归还墨西哥以前的领地得克萨斯、亚利桑那和新墨西哥。但是即使没有这些内容补充，这封电报也已经够重要了，于是蒙哥马利立即把它交给了上司。

1916年10月，为了接任爱丁堡大学校长的职位，攸英已经离开了这个组织。“40号房间”的新主人是海军上将威廉·R·霍尔。当他浏览已被脱密的电文片断时，他十分清楚自己手中拿着的是一份对战争多么重要的文件，一直处于犹豫不决中的美国眼下必须帮助协约国！但这位经验丰富的间谍同时也知道只能十分谨慎地利用这封电报，千万不能让德国人得知英国方面已能读懂他们的密电。

这几天，威尔逊总统府仍在为欧洲作战的和解作最后努力，他对于这封电报的存在还一无所知。1月22日，在参议院的一次演讲中，他呼吁欧洲人实行“不分胜负的和解”。许多美国人也希望欧洲的流血牺牲能最终结束，唯有德国驻华盛顿大使对此不抱任何幻想。伯恩斯托夫已收到齐默尔曼的电报并把它转给了墨西哥城的埃克哈特。图3.2所示为这封加密电报。

担任德国驻美大使8年以来，伯恩斯托夫伯爵一直努力使美国处于欧洲争端之外。1月31日，潜水艇之战爆发前8个小时，他向外交部长罗伯特·蓝辛递交了一份德国政府的有关声明。“我下半辈子讨厌政治！”这位失望的外交官在那天

晚上这么说。3 天之后，美国与德国断绝外交关系。但它仍然保持中立，威尔逊仍然希望他能促成欧洲的和平谈判，而那封未能全部破译的电报也一直搁在“40 号房间”的保险箱里。直到 2 月 5 日，海军上将霍尔才把它交给副国务卿洛德·哈丁。

那一整段时间内，凡是靠近英国岛屿的船都被德国潜水艇击沉，大西洋简直成了船只的葬身之地，德国人相信英国只能在短时间内应付这场无限制潜水艇战，这对吗？

在此期间，洛德·哈丁将电报内容告诉了英国外交大臣阿瑟·詹姆斯·贝尔福，虽然这封电报中有些内容未能破译，但它却足以敦促外交大臣使威尔逊总统得知这一情况。他希望电文的片断已能够动摇美国参战，但他又和霍尔达成一致，认为无论如何也不能让德国人知道在电报的传递过程中出现了漏洞，是否可以设法迷惑他们呢？

海军上将霍尔想出一个计划：设法弄到一份伯恩斯托夫发给墨西哥的埃克哈特的电文副本，如果这封电报中写着另一个日期，却带有伯恩斯托夫的签名，那么在它被公开后，德国人就不得不相信传递途中的漏洞应出在美国或墨西哥的某处。实际上，霍尔是通过一个联络员将这份他所希望的复制品搞到手的，这是一个难以置信的故事，听起来仿佛出自一本拙劣的侦探小说。

墨西哥的某个英国印刷厂老板有一天惊恐地发现他的一名印刷工人在周末用机器制造假钞。在那时，伪造钱币要判处死刑。正当他与他的墨西哥朋友商量该怎么办的时候，那个被发现印制假钞的人为了能让自己逃脱法律制裁，反而将他告到了警察局，印刷厂老板被逮捕并通过即决审判程序处以枪决。值得庆幸的是，这件事发生在周末，而枪决要等到星

期一才能执行。于是这位墨西哥朋友立即向一位名叫H先生的熟人求救，这位H先生为英国间谍机构效力。通过他的关系使英国大使发出警告并插手干预，为印刷厂老板争取到缓刑时间，真正的罪犯被绳之以法。后来，判决被取消，印刷厂老板也被释放，H先生付出的努力取得了成果。从现在起，凡是可能使间谍机构感兴趣的电报，在电报局工作的墨西哥朋友出于感激都会为这个英国人提供副本，这其中也包括这封被破译的齐默尔曼电报的副本。

1917年2月20日，一封与伯恩斯托夫发给埃克哈特的电报一模一样的复制品到了霍尔的书桌上。在此期间，“40号房间”的人经过辛苦工作后破译出了那些缺漏部分，图3.3所示为电报中的一些数字组及与之相应的明文。这时，霍尔可以向英国外交大臣贝尔福宣布，从现在起能够利用这份电报而不会暴露出漏洞在英国。

但是，当威尔逊总统不得不对他如何得知这份电报作出解释时，他该说些什么呢？可以预见，许多参议员都将认为这是一封伪造的电报，难道到那时总统仍不得透露是从英国人那里得到的电文？或者还是应该胡乱找个靠不住的借口？一个美国总统不会撒谎，而威尔逊总统更是从来都不撒谎，霍尔和美国驻伦敦大使想出一个绝妙的办法，当加密电报从墨西哥抵达伦敦的时候，德格雷就带着德国的密本前往美国大使馆，在那儿再一次替这封早已被破译的电文“脱密”。

现在威尔逊总统就能以充满自信的口吻解释这封电报是在美国领土上被破译的——说这话时他一点也没有撒谎。2月24日，贝尔福把电报的内容告诉了威尔逊总统，总统派人进行了调查，因为他想证实这不是一份赝品。在1917年3月1日清晨，人们就已经能够从《纽约时报》上读到：“德国寻求

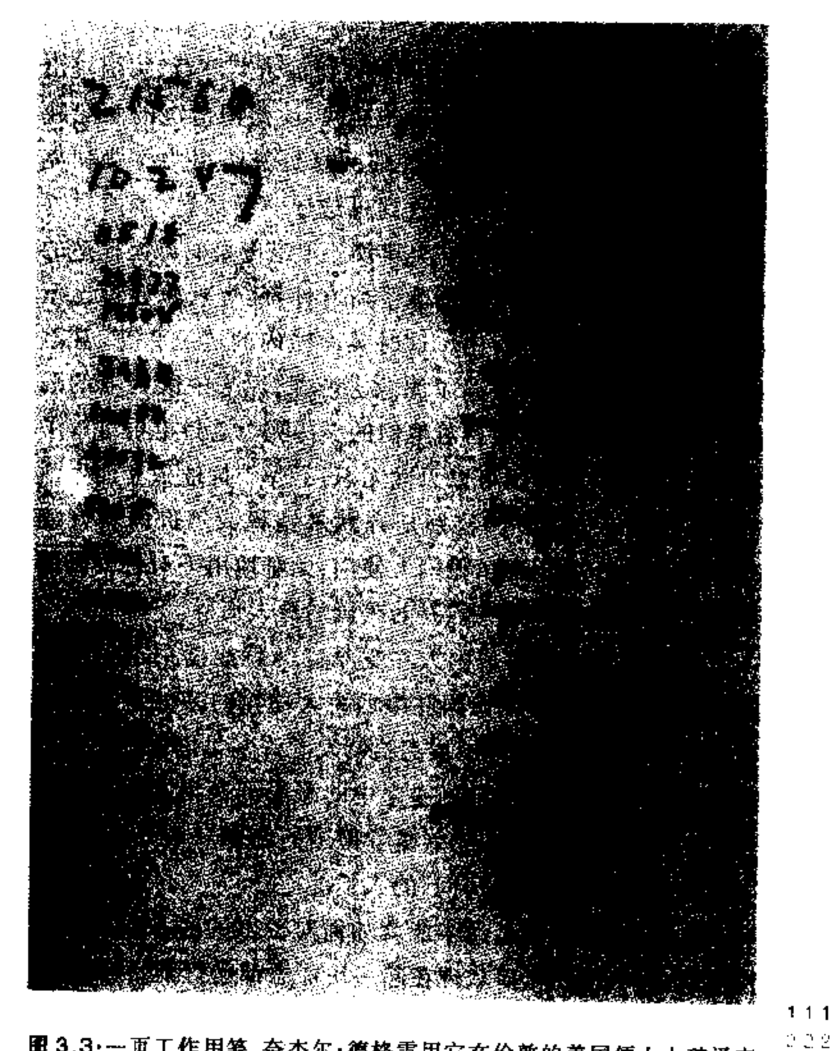


图 3.3：一页工作用笺，奈杰尔·德格雷用它在伦敦的美国领土上破译齐默尔曼电报。

对抗美国的同盟者，并邀日本和墨西哥加入其阵营，德国提出建议的电报已被全篇知晓。”在此期间，被德国击沉的商船吨数已无法估量，但与之相比，这则消息更具吸引力。费利克斯·冯·埃克哈特否认当时曾收到过这样一则消息，墨西哥外交部长也声明从来未得到这类建议。难道电报的确是捏造的吗？一条来自德国的报道消除了所有怀疑：齐默尔曼自己承认编写了电报并将它发出。这时美国国内的情况骤变，甚至连那些德籍美国人都背离了德意志帝国，原来中欧列强的战略家们还一直幼稚地期待着他们的支持呢。这封电报结束了美国人的幻想，即美国可以无忧无虑，不受干扰地独立地生活于世界其他部分之外。特别是齐默尔曼将威尔逊的友好姿态，即将长岛上的电台供德国人使用，无耻地用于对付美国的政治阴谋，人们认为这一点是对美国的极大侮辱。

当齐默尔曼得知美国人在吃早餐时就能读到这封电报后，估计明文肯定是在德国驻墨西哥大使馆的某处落入了他人之手。他十分恼怒地给埃克哈特发了许多封仍采用老方法加密的电报，想了解信息传递途中的漏洞到底出在哪里。显然，他无法想象，敌人已经掌握了德国的密本。而现在，这些电报再也难不倒“40 号房间”的人了。

在此之前，美国人尚未能就如何对德国的潜水艇战作出反应达成一致意见，而从现在起一切疑虑都已打消，1917 年 3 月 17 日，某份杂志中有篇文章的题目就是《齐默尔曼是如何统一美国的》。齐默尔曼电报的破译影响了世界历史的进程。4 月 16 日，美国向德国宣战，此时离德国和奥匈帝国投降还有 9 个月时间。

密本是相当不便于使用的密钥，它一般包括 2000 个左右

的词条，并且不能轻易改换，由于存在落入敌手的危险，还必须不断更新。我们已看到，在轮船上以及在外交部门使用密本有其不足之处，而地面部队利用它则更不安全，因为他们每次都必须带着密本一起转移，所以后来开始采用其他加密方法。与密本相比，人们宁愿采用只需要密钥字的加密方法，因为这些词语可以毫不费力地每天更改。最古老的加密方法之一可以追溯到朱利叶斯·凯撒。

4

他来，他见，他加密

在证实不能指望司令部拿出什么更复杂的方法之后，俄军于1915年采用了一种利用"凯撒"加密步骤的单码置换法。

——弗里德里希·L·鲍尔，《被破译的秘密》

我们知道，"皇帝"这个单词来源于罗马政治家和统帅朱利叶斯·凯撒的名字。在中学时我们就已学过有关他的历史：我来，我见，我征服。我们知道，"剖腹产"这个词也让人想起他的名字，因为据说他就是通过一次这样的手术出世的。然而，鲜为人知的是今天有种加密方法仍被冠以他的名字。

朱利叶斯·凯撒的密码

传记作家苏尔通记载，凯撒送了一封带有秘密内容的密码信给西塞罗，苏尔通十分钦佩地解释道，只有把D读成A，

把 E 读成 B 等等,这封信才能被看懂。图 4.1 所示为这一模式。

a b c d e f g h i j k l m n o p q r s t u v w x y z

图 4.1: 在一字母表下写出另一字母表,把字母往左移几个位置(这里移了 3 位),并在右边空白处写出左边缺漏的字母,于是就得到一张翻译表格,表格的上一行包括了明文字母,下一行为相应的密文字母。

其中上面的字母为明文字母;下面的为密文字母。假如凯撒想用这句话警告一位朋友:

traue nie dem brutus (不要相信布鲁特斯)

那么他会写成:

WUDXHQLH GHP EUXWXV

凯撒的密码就在于将密文字母表与明文字母表相比向左移了 3 位,并将前面的 3 个字母写在右边的空白处。当然,如果不移 3 个字母,他也可以选择移 5 个或 20 个,但总共只有 25 种移法,用第 26 种移法则又得到明文字母表,如果布鲁特斯截获该信并得知密码是通过移动字母表产生的,那么他最迟也可在 25 次尝试后获得明文。

如果不把明文和密文字母表写成两行,而是写在两个可以互相转动的圆盘上,如图 4.2 所示,那么这种移法将更容易理解。外面的圆盘上写的是明文字母表,里面的是密文字母表。开始时使两个圆盘上的相同字母对应,转动(里面的)密文圆盘,如图中所示,以得到这两个字母表的某种对应关系,在这种对应关系中每个明文字母都能找到与之相应的密文字

母。图 4.2 中的字母圆盘不仅对于凯撒式的加密方法十分重要，而且更为复杂的加密也可采用它。因而，美国从事加密工作的政府部门——国家安全局(NSA)——拥有印有图章的圆盘(图 4.3)。今天有谁想破译加密文章，只会对“凯撒密表”付以不屑的一笑。

但尽管如此，现代的加密方法仍保留着凯撒式的痕迹。在简单的“凯撒密表”里，我们已发现两个对于加密十分重要的因素。首先是“规则”，内容如下：“将位于字母表中某个位置上的字母替换成若干个字母之后的某个字母。”学术上常把“规则”称为“算法”。移动的数字，如历史上的“凯撒密表”中的数字 3，是密钥。在“凯撒密表”这种简单的加密方式中密钥就是一个数字。

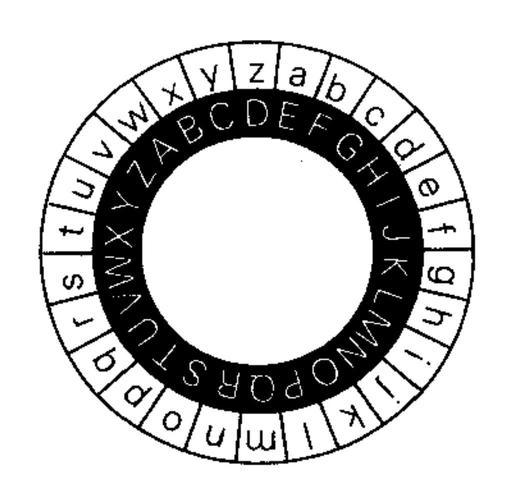


图 4.2：两个可以互相转动的带有字母表的圆盘，与按图 4.1 的方法移动的字母表的作用一样。外面为明文字母表，里面为密文字母表，通过大圆盘和小圆盘的相互转动可以获得所有凯撒式的加密方法。

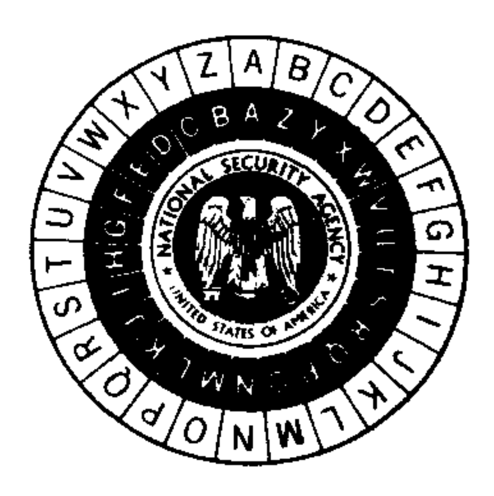


图 4.3:处理加密问题的美国机关"国家安全局"(NSA),为自己选择了一种如图 4.2 所示的加密圆盘。

我们将接触到另一些方法,在这些方法里,密钥为一个单词或者一个单词加一个数字。还有的方法利用整本书作为密钥。我们已经知道的有密本,以及佐尔格的间谍机构使用的统计年鉴。给一条消息加密时,规则和密钥都必不可少,不过,如果想再次阅读这则消息,这两个因素也同样重要。那些只想把自己的信息寄给某个特定部门的人,在使用密钥时就特别麻烦,因为加密和脱密的时候都需要密钥,所以发信人和收信人就必须在某个时间就密钥问题达成一致。而密钥在从一个人到另一个人的传递途中,常常会落入他人之手,如桑道夫伯爵的加密模式,于是被加密的秘密也就不再保密了。

因此,发信人和收信人都采用简短密钥的方法最合适,克劳森的"SUBWAY"就是这样一个例子。我们将在 123 页中看到,一个有妇之夫怎样利用一个密钥字,如用"MAUSI"给他的女秘书寄送加密信件。他能够十分容易地记住这个单词,

不必将它写下,所以可以避免让妻子知道并看懂他的 MAUSI 信,而当他上了年纪记不住这个密钥字时,MAUSI 对他也不起任何作用。我们将在第五章中读到,这个妻子是如何在不知道密钥字的情况下,仍能将这些秘密通信破译出来的。

直到今天,密码学家们还遵循这样一条原则,对密钥保密比对规则保密更为重要。例如德国人在第二次世界大战中使用的叫做"恩尼格玛"的加密机,早在战前就已举世闻名,它的基本模型在那时也可购买得到,它的加密规则是由字母轮和插塞连接构成的。密钥是进行脱密所必须的,也需要保密。它常常在一天当中被更换好几次,这样就使对方还未来得及解开老的密钥,就又面临新的密钥。

a	01	n	14
b	02	o	15
c	03	p	16
d	04	q	17
e	05	r	18
f	06	s	19
g	07	t	20
h	08	u	21
i	09	v	22
j	10	w	23
k	11	x	24
l	12	y	25
m	13	z	26

图 4.4:字母与数字 1 到 26 按字母顺序的对应排列。

让我们依旧回到"凯撒密表"上来吧,如果用数字代替字母,即将字母表中的字母全部编上号,如图 4.4 所示,那么这种方法就更加一目了然了,这样就能将凯撒这句话的明文写

成数字：

20 18 01 21 05 14 09 05 04 05 13 02 18 21 20 21 19

于是密文为：

23 21 04 24 08 17 12 08 07 08 16 05 21 24 23 24 22

现在我们知道“凯撒密表”是如何发挥作用的。将明文字母的数值与密钥数相加，得出加密后的字母的数值，如果结果小于 26，则不存在问题，但是当结果比 26 大时，必须减去 26，取余数。从数值圆盘上看这一点最清楚不过，谁从 A 往下数 27，28 或 29 位，都会得到 B，C 或 D，这与往下数 1，2 和 3 得出的字母一模一样，也就是说，在字母圆盘上计算时，27 = 1，28 = 2，29 = 3，对吗？真是一种奇怪的算法！

用余数计算

我们将在这里碰到一种新的、特殊的计算方法，与日常生活中的计算规则不同，它与数字的大小无关，而与余数有关，即减去某个数字，通常是多次减去这个数字之后剩下的余数，不用多次相减后的余数来确定，也可采用相除后剩下的余数。我们每个人都知道，两个数目相等是什么意思，我们用一个等号来表示它，3 + 4 = 7。但是，除了相等之外，两个数目之间还可能出现另外一种不太紧密的相似之处：它们与第三个数相除后的余数相同。如果我用字母表中的字母总数 26 除数字 27，28 和 29，那么就余下 1、2 和 3，这当然与数字 26 紧密相关。如果我用 17 来除这些数字，余数就为 10、11 和

12。为了避免数字相等与数字的余数相等混淆，我们将在等号上再加上一横，写成 $27 \equiv 1$，但这只限于与 26 相除，所以写成 $27 \equiv 1$（模 26）（读成“关于 26 同余”），与此相应，现在等式 $28 \equiv 2$（模 26），$29 \equiv 3$（模 26）也成立，当然还可以是 $27 \equiv 10$（模 17），$28 \equiv 11$（模 17）和 $29 \equiv 12$（模 17）。

这些数字的余数还表现出一种有用的特性。我们以一组模为 31 的余数为例，这其中如 $40 \equiv 9$（模 31）和 $55 \equiv 24$（模 31）。现在把 40 和 55 相加得出两者之和，即 $40 + 55 = 95 \equiv 2$（模 31），不把这两个数相加并用 31 为模求出余数，我们也可以把它们的余数加起来：$9 + 24 = 33 \equiv 2$（模 31），把这两个数相乘也是一样：$40 \times 55 = 2200 \equiv 30$（模 31）。同样，如果我把余数相乘，也得出：$9 \times 24 = 216 \equiv 30$（模 31）。只要我们对余数有兴趣，都可以用数字的余数相加和相乘代替这些数字的相加和相乘。它的优点在于，能使我们所用的数字不至于太大。

袖珍计算器上的余数

你知道 73 除 95728 的余数是多少吗？你肯定能够十分容易地算出来，把计算器拿出来，用 73 除 95728，结果是 1311.3425。也就是说，95728 中总共包含了 1311 个 73，但是 $1311 \times 73 = 95703$，所以相除后的余数为 $95728 - 95703 = 25$，可以写成 $95728 \equiv 25$（模 73）

但是，这一切与加密以及迫切希望破译信息有什么联系呢？答案是：即使在最先进的加密方法中，计算余数仍然相当重要。但我们还是回到简单的“凯撒密表”上来吧。

带提示词的“凯撒密表”

图 4.2 所示的加密轮中的 25 种排列使 25 种不同的加密方式成为可能，我们可以用简单的方法来为难脱密者，为此我们给密钥“数”加上一个“提示词”，从这个提示词可以引出一个密钥字。因为我们想采用一个尽可能能在脑子里记住的密钥字，所以要求助于一个简单的提示词。

密钥数不必比 26 大，我们以 6 为密钥数，以“Tageszeitung（日报）”为提示词。我们现在分 3 步走：

1. 如果某个字母在提示词中多次出现，那么我们只保留第一次出现的这个字母，其余全部删去。于是从“Tageszeitung（日报）”中得到密钥字：

TAGESZIUN

2. 把明文字母写成一行，从第一个字母开始往右算出密钥数，在我们这个例子是 6 位，然后在下面写出密钥字，如图 4.5 上所示，图中的第二行已有一部分密文字母。

3. 现在从密钥字开始，在空缺的位置上填入其余的字母，当然是按字母的顺序。写到明文字母 Z 下的位置后，继续从前面开始填，结果如图 4.5 下所示。现在我们就得到一行明文字母以及一行为相应的密文准备的字母。

现在我们利用这个密钥，可以把

traue nie dem brutus(不要相信布鲁特斯)

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
.	.	.	.	.	.	*T*	*A*	*G*	*E*	*S*	*Z*	*I*	*U*	*N*	.	.	.	.	.	.	.	.	.	.	.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Q	*R*	*V*	*W*	*X*	*Y*	*T*	*A*	*G*	*E*	*S*	*Z*	*I*	*U*	*N*	*B*	*C*	*D*	*F*	*H*	*J*	*K*	*L*	*M*	*O*	*P*

图 4.5:带提示词的"凯撒密表"。通过提示词"Tageszeitung(日报)"和脱密数字 6 得到明文字母与密文字母的对应关系。

变成

HDQJX UGX WXI RD JHJF

这一方法的原理早在 16 世纪就已被教皇的秘书处所采用。

让我们来仔细观察一下这种加密方法。我们已有密钥数 6 和提示词"Tageszeitung"以及密钥字"TAGESZIUN"。只要不改变密钥,上述明文字母与密文字母的对应关系就总是与原来的相同。E 对应的总是 X。脱密时,每个密文字母都对应一个明文字母,F 总是与 S 相应。人们把这种明确的对应关系称作"单码式的加密"。每个简单的"凯撒密表"以及每个"带提示字的凯撒密表"都是单码式的。

密钥字越长,需要按字母排列顺序填入的字母就越少。从提示词"Tageszeitung"中引出一个由 9 个字母组成的密钥字,因此在第三个步骤中需要填入 17 个字母。从提示词

Donaudampfschiffahrtsgesellschaftskapitaenswitwe

引出密钥字为

DONAUMPFSCHIRTGELKW

所以只需填入 7 个字母。借助越长的密钥字,这种“带提示词的凯撒密表”式的加密方法与简单的“凯撒密表”之间的差别就越大,也就是说,字母的排列顺序越来越无足轻重。如果用《圣经》作为提示词,那么密钥字就已包括了所有的字母,所以不需要再填写任何字母。26 个字母可以在密钥字中任意组合,可以构成如图 4.6 所示的一个密文字母表,但是这样我们就不可能轻易记住所采用的密钥。虽然如此,字母表的任意排列在今天的密码学中仍然起着重要作用。

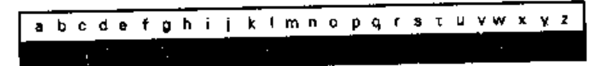


图 4.6:明文字母表(上)与一个随意组合的密文字母表(下)的对应关系。

随意编排的原则

再清楚地解释一遍:在采用单码加密方法时,我们将字母表的 26 个字母按平常的顺序排成一行,然后在下面写出一个任意组合的字母表中的字母,如果想给信息加密,那就在上一行中找出明文的每个字母,并在它的下面找到密文字母。为了能更好地理解这种加密方式,我们必须对这种随意编排的特点进行更为深入的研究。

随意编排的字母表究竟有多少种,答案是令人吃惊的。总的来说也就是:一排东西相互之间交换位置的可能性有多少种。人们很容易确信,A、B 和 C 三个字母能通过 6 种方式进行排列,如果是 4 个字母,就有 24 种可能性,关于排列可能性的数字会如何随着东西数量的增加而迅速递增,还有一个故事呢,这个故事是由奥地利作家埃格蒙特·科莱鲁斯(1888—1939)讲述的:

“在很久很久以前,有一个诚实正直的家庭,家里有父母

和 12 个颇有教养健康成长的孩子。有一天，这家人围着桌子高高兴兴地吃着午饭，突然有个男孩讲起话来，他说，由于他在餐桌旁的位置很不方便，所以总是只能得到剩下的一点汤。这家人相处和睦并已习惯于用和解的方式消除家庭成员间的意见分歧。不久后他们就决定，由于无法让女佣改变围着餐桌服务时的一贯做法，从现在起他们每天变换就餐位置。为了这件事，大家进行了一次谈话，估计需要多长时间才能将所有就餐位置安排的可能性都试遍。'那么，几天，'一个男孩认为。'还不如说几星期呢，'一个女孩冷静地反驳他。最后人们一致认为需要一年时间。'肯定有个相应的公式，'最年长的儿子对大家大声说道……就餐之后，有人拿来了纸和笔，几个大孩子涨红了脸开始计算。这个该死的数字……到底有多大？可怕的结果！数字为：87 178 291 200。应该怎样从这几百亿种可能性开始？为此需要多长时间？对了，一年有 365 天！那么我们就用 365 来除，再次进行计算……'我得出……数字 238844633，'——'你知道，这意味着什么吗？'儿子中的哲学家惊讶地大叫起来，'这意味着，如果我们想试遍所有可能性的话，要到 2.39 亿年以后才能完成我们就餐位置的轮换……'——'那我还来不及得到一份像样的汤就已经死了，'最小的孩子一脸茫然地埋怨着。"

按照故事中谈到的公式，这个由 14 人组成的家庭通过将数字 1 到 14 分别相乘，得到了他们所希望的就餐安排的可能性的总数。

将字母表中的 26 个字母随意编排成密文字母表的可能性有多少？如果一个不走运的收信人收到一封重要的密码信，不小心把他的密钥字母表弄丢了，他应该在多少种可能随意组合的字母表中寻找？每个地球居民，无论是老人或小孩，

都能创造一个只属于自己的密文字母表吗？现在我们必须将数字 1 到 26 分别相乘，可能出现的密文字母表的总数不在 10 亿的范围之内，它大大超过了 10 亿：

403 291 461 126 605 635 584 000 000

在由 50 亿人组成的世界人口中，每个人都可使用 8 亿亿种自己的密文字母表。

排列：

从一种顺序转换成另一种顺序，像洗牌一样，叫做“排列”。如果我们将一副斯卡特牌中的每一张牌都编上号，那么洗牌后，也许 1 号牌在第二十五位，2 号牌在第十三位等等。在这里顺序也被改变了，即进行了“排列”。我们在前面已看到，字母表中 26 个字母排列的可能性总数有多大，而对于 32 张牌来说，可能性则更多得多。

如果我们想更仔细地观察字母表排列的可能性，首先就会被这些无比庞大的可能性总数难倒。如果我们的字母表只是由几个字母组成的，那么一切将会简单得多。

设想我们生活在一个世界里，那儿的居民尚未将字母表中的字母发展到像我们今天所使用的这么多，或许仍停留在 4 个字母上，例如 A、B、C 和 D。这 4 个字母共有 24 种排列形式，在图 4.7 中都已列举出来。从 ABCD 可以通过排列转换成 DABC，图 4.8 的左上所示为一种排列到另一种排列的变换过程。将 A 换成 D，B 换成 A，C 和 D 换成 B 和 C，我们给这种排列取名为 X，它将 ABCD 转变为 DABC。右边所示为另一种排列，我们称之为 Y，它把 ABCD 这组排列变为 BDCA。

就像能反复多次洗一叠牌一样，我们也能任意依次完成多种排列。图 4.8 第二行就通过排列 X 从 ABCD 产生出

DABC,再通过排列 Y 从这组排列中产生出 ABDC,于是依次完成排列 X 和 Y 后,又可得到一种新的排列,如图下方所示,不过小心!谁想依次进行几种形式的排列,必须注意先后顺序,因为如先采用排列形式 Y,然后采用 X,则得出另一种排列。于是从 ABCD 变成了 ACBD。

ABCD	ABDC	ACBD	ACDB	ADBC	ADCB
BACD	BADC	BCAD	BCDA	BDAC	BDCA
CBAD	CBDA	CABD	CADB	CDBA	CDAB
DBCA	DBAC	DCBA	DCAB	DABC	DACB

图 4.7:字母 A,B,C 和 D 的不同排列

X: A → D, B → A, C → B, D → C

Y: A → B, B → D, C → C, D → A

X Y: A → D → A, B → A → B, C → B → D, D → C → C

Y X: A → B → A, B → D → C, C → C → B, D → A → D

XY: A → A, B → B, C → D, D → C

YX: A → A, B → C, C → B, D → D

图 4.8:排列方式 X 和 Y(上)。图示的意思是,方式 X 为:A 换成 D,B 换成 A,C 换成 B,以及 D 换成 C。Y 则相反:A 换成 B……依次完成排列 X 和 Y 后,得到一种新的排列。但这取决于单个排列方式的先后顺序。如果先按 X 要求的方式进行排列,接着按照 Y 排列(中左),将得到一种与先按照 Y 然后按照 X 方式排列得出的结果(中右)所不同的字母排列。XY 和 YX 这两种合成的排列方式如该图下方所示。

假设我们已通过一个经过排列的字母表将一篇明文制成一篇密文。如果我用另一个任意组合的字母表将它再次加密,它会变得更加隐秘吗?脱密会因此更难吗?如果我将一篇文章进行50次加密,每次都采用一个不同的经过排列的字母表,这是否会给一个窃码者造成无法克服的障碍呢?他既不知道我这50个不同的经过排列的字母表,又不明白我是按照什么顺序依次进行排列的。——不,先后进行50次排列并不比一次更强!不管我先后进行了多次排列,最后的效果总与唯一的一种有关,这并不奇怪,即使将已洗好的牌再洗,2次或5次或更多次,也同样不会把它们洗得更好。

在许多方面,事物的排列,无论是纸牌或是字母,都可与数字的相乘进行比较。依次进行两次或50次排列或相乘,都可用唯一的一次来代替。谁将一个数先与3然后与7相乘,都可以将它直接与21相乘。先后两次相乘可以仅仅用一次来代替。但是,无论我先与3后与7相乘或先与7后与3相乘,结果都一样,而在排列时却与先后顺序有关。

排列的倒数

排列与乘法还有另一种相似之处。如果我把5与7相乘,得出35。如果我把结果与1/7,即与7的倒数相乘,则又回到5。每个乘法都有一个"反乘法"与之相对,即与倒数相乘,如果我依次进行乘法与"反乘法",则看起来似乎我把原来的数字乘了1一样。

如果我还提出一种排列,把A换成A,B换成B,那么人们可能会认为这是一种幼稚的行为。尽管这样,我们还是仔细来分析一下并把它称之为字母E。它已

在图 4.9 右下表示出来了。这种排列与乘法中的 1 相符。

如乘法中一样，每个排列也有另外一个取消它的作用的排列。图 4.9 上面的排列 X 旁还有另外一个排列，我们称之为 1/X。它表示 X 的“倒数”或 X 的“反排列”，正如乘法中 1/5 为 5 的倒数(或逆值)一样。人们很容易确信，无论采用何种先后顺序，X 与 1/X 总是与 E 一样，不会引起任何变化。所以，如果我们通过某种排列方法将字母表转换成另一种顺序，反排列将会恢复字母表原来的顺序。

X: A → D, B → A, C → B, D → C

1/X: A → B, B → C, C → D, D → A

A → D → A
B → A → B
C → B → C
D → C → D
X 1/X

A → A
B → B
C → C
D → D
E

图 4.9：排列 X(左上)和它的倒数(右上)。一个取消另一个的作用。先后进行 X 和 1/X 这两种排列，将与排列 E 一样，不会引起任何变化。

然而实际上我们字母表中的字母不止 4 个，而是 26 个。利用图 4.6 中的表格加密是以明文字母表的某种排列为基础的，即将顺序 a、b、c、d……排列成密文字母表 P、D、N、Z……每个“凯撒密表”和“带提示词的凯撒密表”也都是一种排列。图 4.6 中的密钥表只不过是将明文字母表转化为密文字母表

的一种排列而已。字母表的每一种排列都会产生一个密钥表。如果我们在由 4 个字母组成的字母表中，通过图 4.9 中的排列 X 将 ADAC 加密，将得到 DCDB，利用反排列，即利用 1/X 就能进行脱密。很容易证明，这种排列使 ADAC 又重新显现出来。

当然，进行单码式的加密，除字母外也可任意采用其他符号，如数字、纸牌或多米诺骨牌，但其中对应同一类字母总是必须采用相同的符号，每种单码式的加密方法都包含一个类似图 4.6 的密钥表，脱密时就将密钥表“倒过来”看。

可能产生的密钥表的总数虽然很大，但却是有限的。原则上可以借助电脑破译一篇已被加密的文章，按顺序将可能出现的无以数计的密钥表全部试遍并检查，是否从其中可以产生一篇有条理的文篇。但实际上这却是不可能的。假如电脑能够将有意义的文章与无意义的文章区分开来，并且只需千分之一秒就可完成一个密钥表的检验工作，那么要将所有可能性一一尝试，仍需要一段远远超过宇宙年龄的时间。因此，通过简单的试验来寻找正确的密钥表是毫无希望的。

但是，没有哪一种加密方式是真正保密的。假设我们有一个由 10 个字母组成的密文。如：

JCPRTETZTM

像每次加密一样，每个密文字母都对应某一个明文字母，明文也是由 10 个字母依次排列组成的。通过多少种方式可将字母表中的 26 个字母概括成 10 个字母？要找的数是一个

1和26个零。即使这个数字是我们无法想象的庞大,它也是有限的。设想一下,我们有一台电脑,它可以将所有由10个字母组成的排列顺序依次分行写出,于是这其中肯定有正确的明文,困难在于把它从多如牛毛的10个字母的组合中找出来。哲学家、数学家和科幻小说家库尔德·拉斯维茨在他的短篇小说《大百科图书馆》中对这个思考过程进行了进一步的发挥。他选取的不是10个字母的组合,而是全部书籍,大百科图书馆应该包括所有原则上能写出来的书籍。

这个想法很简单。我们以一本德语书为例。我们有26个字母,另外还有变音,β,然后是标点符号、单词间的空格、10个数字,而且可能还有几个用于科学论文的希腊文的和数学的符号。假设我们总共有50个不同符号。我们图书馆里的书应该有600页之多,而且每页包含3,300个符号,如果哪本书比这短,我们就用空格号来补充。于是每本书都包括1,980,000个符号,每本书都是由50种符号组成的,这50种符号不断以新的排列方式反复出现。所以我们这50种不同符号与1,980,000这个符号组编排的方式可能有多少种,大百科图书馆就可能有多少本书。因此我们有50×50×50×……种不同的可能性,在这个过程中,我们其实应该写入1,980,000×50种,结果是一个由三千万位数组成的数字。这成了一个浩如烟海的图书馆,而图书管理员早就不得不走完的书架间的距离使得我们与最遥远的星系间的距离都变得微不足道了。这其中绝大部分书中都只是些毫无意义的符号组,但如果用足够长的时间寻找,也会在所有毫无意义的书籍中发现用空格符号补充过的《路德圣经》以及《基本法》的文本。也可能突然在某处发现歌德的《浮士德》和卡尔·迈的《温内托》。但是在这个图书馆里不仅能找到所有已出版的文本,

而且还能找到所有以后要写的书籍。也许今天你就能在那里阅读会使你的曾孙一举闻名的博士论文。

这种图书馆实际上是不存在的,原因在于它超越了地球上所有可采用的手段的极限——材料、空间和劳动力。然而即便存在这个图书馆,它也无用武之地,谁有能力在无以数计的毫无意义的书籍中找出一本书来,至少这本书在语言上是对的——尚且不管它的内容如何?

回到我们的加密上来,那些需要花上几千年时间进行系统性的尝试才能获得明文的方法,在今天仍被大加赞扬。德国人在第二次世界大战中认为,他们可以依赖他们的加密机“恩尼格玛”。因为要破译密文,必须进行无法想象的多次试探。然而这种想法是错误的,我们将在下一章节中看到,在不知道密钥的情况下人们不依赖毫无计划的试探。

一台多余的机器

对一条信息进行加密和脱密非常简单。我们只需一张如图 4.6 所示的纸条,就肯定能通过它将明文转化为密文或者相反。但我们仍希望能设计出一种能自动完成这些工作的电动机器。像操作打字机一样,使用者只要在一个键盘上按一下某个带有明文字母的按键,一盏标志密文字母的小灯就会亮起来。当然也可以接上一台能立即把密码字母打印到纸上的电动打字机。由于关键的只是原理,所以我们该满足于这盏会发光的小灯了。

读者会问自己,为什么非得为了一件这么简单的事情设计一台仪器呢?原因在于,这样我们就能够理解简单加密机的原理。在接下来的几章里我们还将使这台机器不断扩大。

这里设计出的这台小仪器从真正意义上来说，只是第二次世界大战中德国加密机“恩尼格玛”这台大型装置上的一个小轮子而已。为了能一目了然地观察，我们再次把自己限制在由4个字母组成的字母表中。

我们需要为这台机器找4个小白炽灯、4个电动开关和一个板坯，这是我们可以自行建造的仪器的“心脏部分”。当然你现在不必去拿钢丝锯和烙铁，因为你根本不用制作。我只是认为，最好用一种施工说明的方式来描写这台仪器的制造过程。板坯是一个由柔韧的绝缘材料制成的长方体——硬纸板就行——在长的一边分别有4个位置相对的电子接触点。现在，用一条电线将左侧的每个接触点与右侧的某个接触点连接起来。总共有24种不同的连接方式，我们就选择其中的一种。现在我们利用开关，白炽灯和刚才做好的板坯来制作一个电子电路系统，如图4.10上方的图表所示。每个开关都与一个明文字母相对应（右），而每盏灯都对应一个密文字母（左）。白炽灯和开关与一节电池连接在一起，如所有开关都被往上提起，则未接通任何电路，所有灯泡都不会亮。现在我们按下开关C，经过灯泡D的电路就接通了。所以明文字母C与密文字母D对应。利用图表，你可以较容易地看出存在下列对应关系：a一C，b一A以及d一B。于是板坯的电路装置就与图中右上的加密图相符。我们可以利用图4.10下所描绘的机器来脱密。我们按下与密文字母对应的开关，表示明文字母的灯泡就会发光。

如果我们拿出26个开关和26盏白炽灯，并用电线将板坯上左边的26个接触点与右边的26个连接起来，那么就会得到一个相当于图4.6中的加密条的机器，不过也是按照不同的单码式加密方法进行工作的。同样，每个加密图都准确

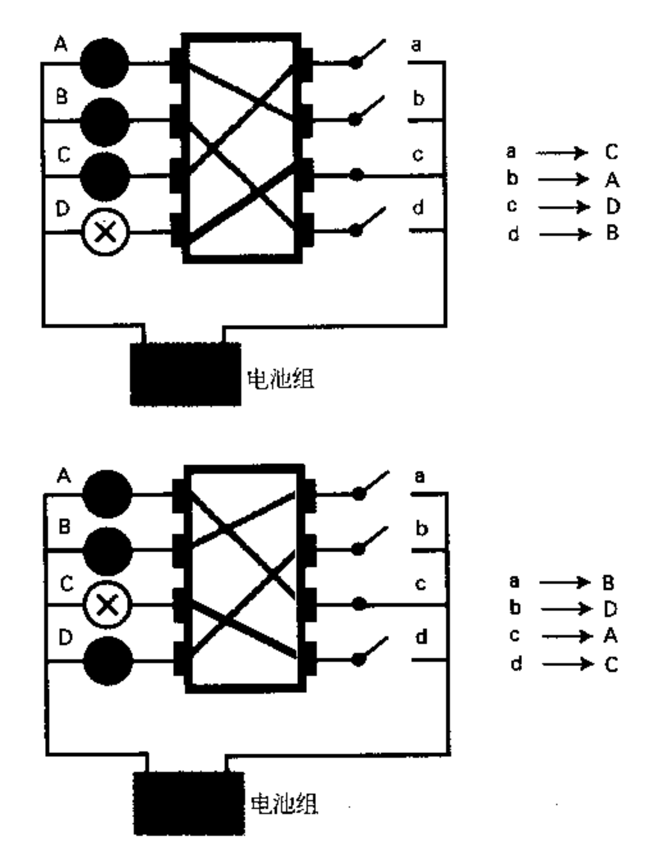


图 4.10:利用一个电子电路系统编密。a、b、c、d 4 个开关可使 A、B、C、D 4 个灯泡发光,为此只要将开关上的明文字母打入,依次发光的灯泡就连成了由此产生的密文。其右所示为通过这个电路装置得出的字母表排列。图下:用来破译按照上述排列制成的密文的电路装置。打入相应按键上的密文,与明文字母对应的灯泡就会亮起来。右边所示为对应的字母排列,它是位于它上方的排列方式的反排列。

地对应一个电路装置,反之亦然,如果我们想脱密,必须利用一个板坯,其原理与原来图中下面部分所展示的通过 4 个字母的字母表制成的板坯原理一模一样。而与上面不同的是这

时开关对应密文字母，灯泡对应明文字母。

当1915年左右出现电动打字机时，人们首次成功地利用电动机器加密。使用这种机器时，只要按下一个键，即一个接通电源的开关，它就会通过电磁带动装有铅字的连动杆将铅字印到纸上。在普通的打字机上，按a键就会带动连动杆a，现在通过改动电路装置可以使c键与连动杆a，d键与连动杆b等等对应。这样机器就自动地将打入的明文转化为密文。不过它只能提供一种单码加密方式。

如果今天的脱密者碰到这样一种加密方式，他将喜出望外，因为他在转眼之间就能将其破译。人们是怎样来对付这种密文的，埃德加·爱伦·坡笔下的英雄威廉·莱格兰德和大名鼎鼎的歇洛克·福尔摩斯早就知道了这一点。

5

如何破译单码加密

在德语中，引人注目的是 e 高踞其巅，n 可视为峰，f、g、h、i 为山体侧面连接 j－k 低地，o－p－q 的山谷连接 r－s－t－u 的山脊。

弗里德里希·L·鲍尔《破译的秘密》

他们找到了螺栓，开启箱子就不费吹灰之力了。金银珠宝在灯光的映照下，熠熠闪光，莱格兰德欣喜若狂，而他的黑人随从，丘辟特的脸色变得如此苍白，可以说已到了此类肤色人种的极限。他跪倒在墓坑中，双臂深深地插入到财宝中，直没到肘弯，然后停住不动。这两个人发现了基德船长的宝藏，基德船长是从前在海上兴风作浪的苏格兰海盗。

这则故事是杜撰的。美国作家埃德加·爱伦·坡（1809—1849）于 1843 年发表了它，题目是《金甲虫》。故事讲述了怪人威廉·莱格兰德在海滩捡到一张羊皮纸，上面是一篇单码密文。莱格兰德成功地破译了它，从中获悉了基德船长藏宝地，

150年前,基德船长被谋杀了。

埃德加·爱伦·坡破译密文信件

爱伦·坡的小说在两方面值得重视。一方面因其锋刃般锐利的逻辑推理而卓然出众,成为现代小说的先驱。另一方面坡的笔墨所及,刻画了病态心理和超自然现象,诡谲而恐怖。小说《金甲虫》综合了上述两个方面,其中有神秘的海盗财富,包括粗大的耳环、指环以及抢来的金表。而更可怕的是引导人们找到财富的那些指示。其中有一样东西,人们必须让它穿过钉在一棵树上的一个死人头颅的左眼落到地上,它才能指出地上的那个正确位置。莱格兰德用分析逻辑的方法破译了手稿,今天我们解单码密码也是用分析逻辑。

研究密码学是作家的癖好。1839年,他在一本杂志中,评价了猜谜,尤其是脱密的价值。他力邀读者编撰单码密码,并将加密的文章寄给他。回音并不需要等很久。其中有一篇密文出自17岁的斯凯勒·科尔法克斯之手——他后来当选为美国的副总统。

坡破译了收到的绝大部分密文。他发现,其中有两篇不能算是真正意义上的文章,而是由符号任意排列组合而成。还有一篇没有按照坡要求的那样,由26个与字母表相对应的符号构成,而是有51个,因而根本不能算是单码加密。密文如潮水般涌来,而坡几乎全都成功破译,这使他声名大震。据目击者说,有时他破译一篇密文,只需要别人加密时间的一小部分。人们猜测,坡在解密方面的成就主要基于直觉。而关于密码学的一个最重要的辅助方法,他却是以后从百科辞典中获知的。

字母表中的单个字母在每一种语言中的出现频率都不同，这种频率是具有代表性的。在德语、英语、法语、意大利语和西班牙语中，字母 e 最经常出现，而葡萄牙语中则是 a，德语和英语中，q 是最少出现的字母，其他语言中则是 w。坡赢得了解密天才的美誉。他对自己的方法注意保密，以保住这一光环。不过在《金甲虫》的故事中，他还是运用了自己的知识，故事中密码学家坡对作家进行口授。这篇写在基德船长羊皮纸上的密文见图 5.1。让我们追随坡笔下的主人公莱格兰德，看他是怎样从密文中得到明文的。

53≠≠†305))6*;4826)4≠.)4≠);806*;48†8¶60))85;1≠(;:
≠*8†83(88)5*†;46(;88*96*?;8)*≠(;485);5*†2:*≠(;4956*
2(5*—4)8¶8*;4069285);)6†8)4≠≠;1(≠9;48081;8:8≠1;
48†85;4)485†528806*81(≠9;48;(88;4(≠?34;48)4≠;161;:
188;≠?;

图 5.1：埃德加·爱伦·坡的小说《金甲虫》中基德船长的密信

在羊皮纸的一角上，一只小山羊的图形清晰可辨。山羊的英文名称是“Kid”，德语中相应为“Kitz”，再考虑到自己发现羊皮纸时的情形，莱格兰德断定，这篇东西肯定与海盗基德船长的一则消息有关。由此可以推测，明文是用英语写的。接着莱格兰德统计了单个符号的出现频率。8 共出现33次，远远超过其他符号。莱格兰德推断，8 代表 e，并进一步断定，8 的 5 次成双出现，即对应英语中的“ee”。在单码密文中，最常见的单词“the”必然表现为一个重复出现的字母组合，它应由

3个字母组成，并且以8结尾。事实上，由3个符号组合的；48共出现7次。于是莱格兰德尝试用；代替t，4代替h。我们再来看倒数第三十三个符号，那儿一开头是“the”的3个符号组合；48，接着是一个t，之后有一个暂未确定的符号(，再接下来是两个e，一个t和一个h，也就是“t.eeth”。现在，我们浏览整个字母表，为“t.eeth”中的空格寻找一个合适的字母，然而无论如何也得不出一个英语单词。因此，莱格兰德认为，“th”这两个字母应属于下一个单词。这样就剩下了“t.ee”。他再次查阅字母表，试图找到可以代替(的字母。结果断定，只有采用r的时候，可以得到某种意义。由此得到的单词是“tree”(树)。由此可见，这一组密码很有可能是“the tree”。接着我们可以辨认出下面3个字母，即“thr”，接下来是3个我们还不认识的符号≠?з，同它们相接的是一个“h”和单词“the”。于是，我们得到了“the tree thr…hthe”。“thr…h”，讲英语的莱格兰德很自然地联想到单词“through”。

如果这项假设成立，那么接下来的3个符号≠，?和3分别对应字母ou和g。于是我们发现，第二行开头的一个组合+83(88，应是“.egree”，莱格兰德推断，这个词肯定是“degree”，即“程度”的英文。那么符号+应代表字母“d”。“degree”之后5个符号是字符组合；46(；88。借助已破译的符号，可以得到“th.rtee”，这只有可能代表“thirteen”，即“13”。由此推出，符号6和*分别代表字母“i”和“n”。至此，莱格兰德用明文字母代替了所有可以辨认的密符。但是这封信依然不通，不过莱格兰德还可以继续猜下去。这封信开头的符号是53≠≠+，运用已知的译释，我们可以得到“.good”。在英语中，由一个字母组成的单词寥寥可数。几乎可以肯定，5应用“a”译释。那么这条消息是以“a good”开头的，即“一个好的”。

莱格兰德就这样逐个字母揣摩，最终他读懂了这段文字，翻成德文是，"魔鬼领地主教客栈中的一只好的望远镜，东北 41°13'，东面第七根枝桠的北向树枝，从 50 英尺外笔直向树发射，穿过死人头颅的左眼。"

这则密信依然令人费解，不过这已不是密码学家的任务了。接下来需要通过侦探的努力来解释它。

魂归西天的基德船长还给解密者增设了一个障碍，他把所有的符号并列在一起，不设字空隙。假如他通过字空隙或某个固定的符号，将每个单词的范围表示出来，那么莱格兰德破译起来就容易多了。

歇洛克·福尔摩斯和跳舞小人

事情到了歇洛克·福尔摩斯这里就变简单了。在阿瑟·柯南道尔的小说《跳舞小人》中，阿贝·斯莱尼这个"芝加哥最阴险的骗子"，向他年轻时代的恋人埃尔西发出了威胁信号。埃尔西眼下住在英国，而且已嫁给一位大庄园主。他用的密码是两人以前使用的：他在庄园的窗台、工具棚门等处用粉笔画了许多各种姿态的跳舞小人，而且他在庄园附近租了一个房间。埃尔西希望，对于自己的过去，丈夫知道得越少越好，而庄园主对魂不附体的妻子和一再出现的图形深感不安。他将这段时间内在庄园里发现的人形密信临摹下来，并交给了歇洛克·福尔摩斯。图 5.2 中的前 6 行，就是大侦探在破译时使用的所有密文。

几个小人手中举着旗子，使大师灵机一动。歇洛克·福尔摩斯马上推断，这些小旗暗示了某种字义。接下来的思路同莱格兰德如出一辙。有一个小人在密文中最常见，它分腿而

立,两臂上举。福尔摩斯断定它代表字母 e。很快,福尔摩斯就把小人与绝大部分字母对上了号,最后他自己也可以利用这一体系给简单的信息加密了。他已从斯莱尼的密信中知晓其住处,于是寄给他一封自己加密的信,内容是:"come here at once(马上来吧)"。这是图 5.2 中最后一行的意思。斯莱尼以为这是他的意中人所为,他在不知不觉中落入陷阱。伟大的歇洛克·福尔摩斯又一次取得了胜利!

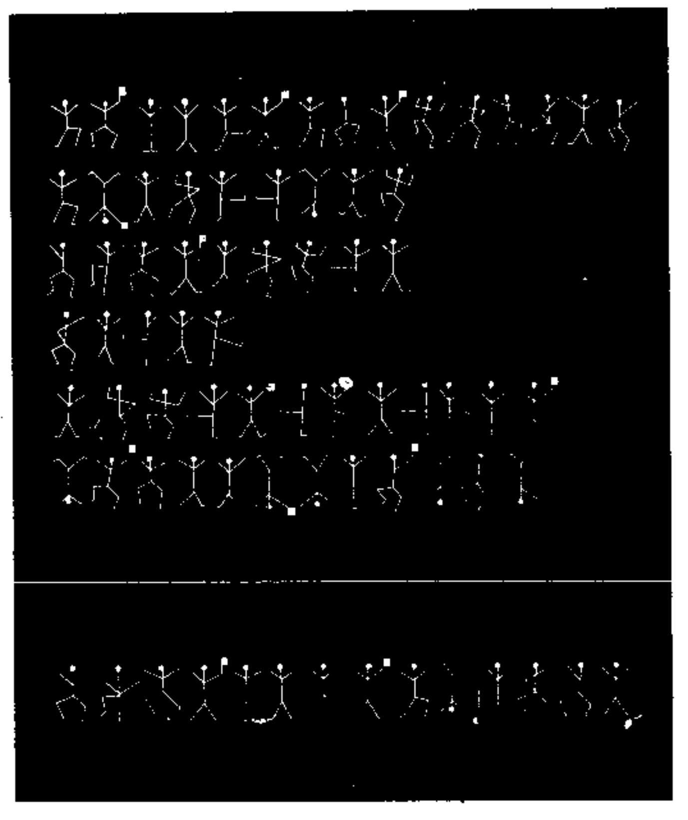


图 5.2 上:小说《跳舞小人》中,供歇洛克·福尔摩斯使用的密信。下:大侦探成功地破译密码之后,回寄给作案者的密信。

以上从文学作品中撷取的两个例子体现了某些规则，遵循它们，我们就可以破解单码密文。两例均源于英语明文，但在德语中情况亦无甚差异。

然而我们在为德语单码密文脱密之前，还应该装备一些行之有效的工具。

频繁的 e 和稀罕的 q

同英文一样，德文中字母的使用频率也有差别。在一篇文章中，单个字母出现频率的规律性令人惊异，无论是康德《纯粹理性批判》还是爱情小说。虽然这涉及到一种统计的规律性，但在达到一定篇幅的文章中，这种规律性则极少出现偏差。与英语相同，在德文中出现最频繁的字母，依然是 e，当然这只适用于较长的文本。"staubsauger（吸尘器）"并不能算一个反例，只要我们将其放入一篇较长的文章中，就会发现，e 出现的次数比 a 和 u 多得多。

在图 5.3 的表中，可以看到字母表中的所有字母在德语文章中出现的频率百分比。[①] 这里，变元音 ä、ö 和 ü 分别用 ae、oe、ue，β 则用 ss 代替。图 5.4 以图块形式，再次显示了这种分配比例。我们看到，e 和 n 是最常见的字母，接下来是 i、s、r、a 和 t。

只要搞清楚哪个符号代表 e，就可以顺着字母对这条线索，继续探寻密钥字母表。德语中出现最频繁的字母对是 en 和 er，接下来是：ch、te、de、nd、ei、ie、in 和 es。在字母 e 打头的

① 图 5.3 表格参见阿尔布雷希特·博伊特尔施帕赫尔所著的《密码学》，不伦瑞克，1993 年（第 3 版），第 18 页。图 5.4 中的图示亦参照此绘制。

成双的字母组中第二个字母按出现频率顺序排列的是:n、r、i和s。

a	6.51	n	9.78
b	1.89	o	2.51
c	3.06	p	0.79
d	5.08	q	0.02
e	17.40	r	7.00
f	1.66	s	7.27
g	3.01	t	6.15
h	4.76	u	4.35
i	7.55	v	0.67
j	0.27	w	1.89
k	1.21	x	0.03
l	3.44	y	0.04
m	2.53	z	1.13

图 5.3:德语字母表中字母的频率分配,以百分比计。

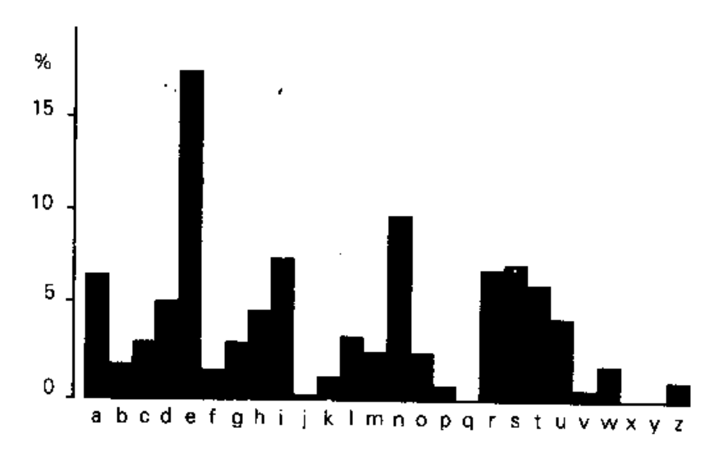


图 5.4:图系德语中字母出现的频率分配。其中涉及到第五章开始弗里德里希·L·鲍尔提到的词。

另外，德语中的一些单词也以不同的频率出现，而且这种频率性几乎是所有文章的特征。下面是一些最常见的短词，依次为：die、der、zu、in、ein、an、den、auf、das。尤其在脱密时，如果密文能让人识别其词的分隔，它们对脱密会很有帮助。

德语中哪个名词使用得最多呢？是钱（Geld）还是“马克（Mark）”？是“汽车（Auto）”还是“电视（Fernsehen）”？都不是，“时间（Zeit）”遥遥领先，其后是“先生（Herr）”和“年龄（Jahre）”，“女人（Frau）”居第十四位。“马克（Mark）”则处在第十六的位置。毕竟它还是排在“上帝（Gott）”的前面。

破译密码文

现在，我们先来挑战一篇简单的密码文。说它简单，是因为文章的单词间有字间距空隙相隔，人们马上就可以辨认出，哪些是短词，这的确非常方便，我们很快就可以体会到。图5.5是一篇单码密文：

FB EMG GMLMQ CJMBLP HJB HFP CKMBCSFL
JB EMG DMQP RJPP SK DMGEMB JIMG HFP
RMANSFL FRP EFM DMQP HKMEM JB KBR LMDOGEMB

图5.5：一篇密码文。

这篇文章中共使用了19个不同的符号。如果将它们出现的频率归纳起来，可以得出下列结果：

M(17,18.0%)	E(6,6.4%)
B(9,9.6%)	G(6,6.4%)
P(8,8.5%)	J(6,6.4%)
F(7,7.4%)	L(5,5.3%)

括号中是每个符号在文章中出现的次数，以及换算成百分比的出现频率。

据此人们推测，M这个符号应同明文字母e对应。事实上，在图5.3的表格中，字母e的出现频率就接近18%。接下来我们看密文中一些由3个字母组成的单词。EMG共出现了两次，一个由3个字母组成的词，其中e处于中间位置。最常见的3个字母的短词，而且e处于中间，就我们所知有der和den。在这两种情况中，E似乎同d一致，但G究竟对应r还是n，却依然悬而未决。这里，字母对的知识也帮不了我们的忙，因为er和en都很常见。我们将视线转向3个字母的单词EFM，这个词中有两个字母已知，第一个是d，最后一个则是e。有关最常见短词的常识告诉我们，这个单词很有可能是die，于是我们又得到一个字母，F对应字母i。接下来，篇首单词可以继续向我们提供帮助：这个单词有两个字母，第一个是i，处于第二位的是密文字母B，它在文中出现的次数居第二位。只要我们看一下表格，就会发觉，相应的明文字母似乎应是n。根据这个假设，第一个单词应是in，而第二个词的最后一个符号不可能也代表n，否则处在那个位置上的应是B，而不是G。由此可见，第二个词应是der，同G对应的是字母r。这样，这封信的开头为"in der…"，这听起来也颇合逻辑。接下来看双字母单词JB，它也出现了两次。我们推测明文应是".n"，而"in"是不可能的，也许是"an"，由此看来，J对应a。

现在我们置换密文中已破解的符号。当然，我们还不能确定，我们的译释是否正确，也许我们会因此遭遇困境，就像有人将一个错字填进猜字谜的十字中时，会发生的情况一样。由此我们得到的明文还不十分完整：

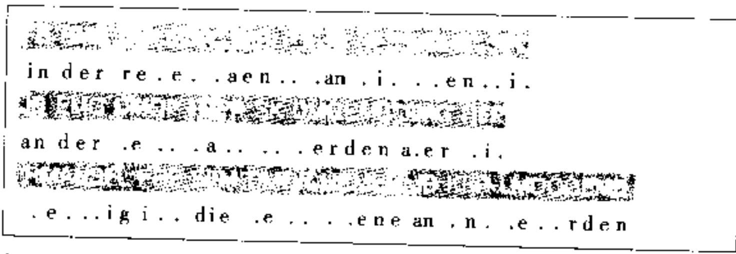


图 5.6:图 5.5 的密文,其中的 e 和 n,我们已借助频率知识作了确认,还有几个字母也借助短词得到确定。

联系前两个词,第三个词中的 L 似乎应对应 g,而与 Q 对应的则是 L。于是,明文这样开始"in der Regel…(通常)"。这也使我们可以在下文中延用 g 和 L 的破译。

现在文中有两个单词,分别缺一个明文字母。第十四个单词暂时为"a.er",它不可能被译成"ader",因为与 d 相对应的是 E,也许会是"aber"? 对此我们必需作进一步探究,因为 I 再也没出现,所以这一项知识不会为我们继续提供帮助。我们现在把视线转向前面一个词,".erden"。它有可能是"herden"或"werden"。我们推测符号 D 应表示 h 或 w,在最后一个单词"ge..rden"中,D 再次出现,而这个单词更可能是"geworden"。至此,我们又得到了两个新字母:D 对应 W,O 对应 O。下面是第二篇明密对照文:

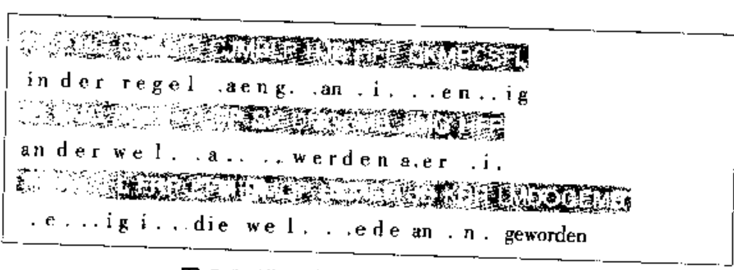


图 5.7:进一步脱密后的图 5.5 密文。

现在我们把第五个单词“.an”提出来。事实上只有“man”合适。倘若无误，我们有4次机会用m来代替H，结果看来是有意义的。“mi.”共出现了两次，但它不可能是“mir”，因为代表r的是G。于是我们推断其为“mit”。P可能对应t。这样我们就能置入其他字母。现在再来看前6个词：“in der Regel.aengt man mit”。从图5.8可以看出，我们的破译工作已进行到了哪一步。

那么第四个单词究竟是“faengt”还是“haengt”呢？7号词不可能是“huenh.ig”，因为“fuenf.ig”更合理些，由此推断：C是f，S为Z，剩下的问题就是顽童也可以解决的了。我们来看第十一个词“.att”，到底是什么呢？“matt”，“satt”，还是棋手使用的“patt”？可它既不可能是“matt”，也不会是“patt”，因为这样一来倒数第二个词就变成以“nm”或“np”结尾了。而如果“satt”成立，那么得到的词尾是“ns”，这看起来完全符合逻辑，由此我们也得到了倒数第二个词。是“ins”，“ans”，还是“uns”？因为a和i都已确认，所以它只能是u。至此一切都豁然开朗：“in der regel fae ngt man mit fuenfzig an，der”——完全正确，接下来是什么呢？从“fuenfzig”一词中我们已确认，S对应Z。于是我们得到了隐含于其中的格言：

```
HJ EMG GMLMQ CJMBLP HJB HFP CKMBCSFL
in der regel .aengt man mit .uen..ig
JB EMG DMQP RJPP SK DMGEMB JIMG HFP
an der welt .att ..werden a.er mit
RMANSFL FRP EFM DMQP HKMEM JB KBR LMDOGEMB
.e...igi.t die welt m.ede an .n. geworden
```

图5.8：破译接近完成的图5.5密文。

"in der regel faengt man mit fuenfzig an
der welt satt zu werden aber mit sechzig
ist die welt muede an uns geworden"
(通常人们在 50 岁时开始厌倦尘世,而到 60
岁时,世界却已对我们忍无可忍)

破译单码密码,不只有一种方法。也许您感到自图 5.6 之后,我们的步伐有点太草率了。当时我们推测第三个词为"regel",并由此得到了两个新字母,其实我们还可以走别的路。让我们再从这个残篇开始,尝试着暂时不用第三个词,转而观察第五个单词。这个词由 3 个字母组成,其中两个已知。那么".an"会让我们联想到什么呢?可能是"man"。我们试着用 m 代替 H。现在文中又出现了一个 3 个字母的单词"mi.",这第三个字母是什么呢?

我们翻开杜登百科辞典(解密者可以使用任何工具),发现这个词可能是"mia","mia"一般被用作 Milliade(百万)的缩写形式,或是 Maria 的昵称。不过,也有可能是 Million 的缩写"mio",Minute 的缩写"min",或"mir"及"mit"。"mia"、"mir"和"min"的可能性可以排除,因为它们的第三个字母 a、n 和 r 都已确认。那么 P 还可以代表 O 或 t。假设 O 成立,那么倒数第七个词为"i. O"。照此推理,我们在第二行得到一个".aoo"——更糟糕。然后我们试着用 t 代替 P,并把目前已知的字母写进去:

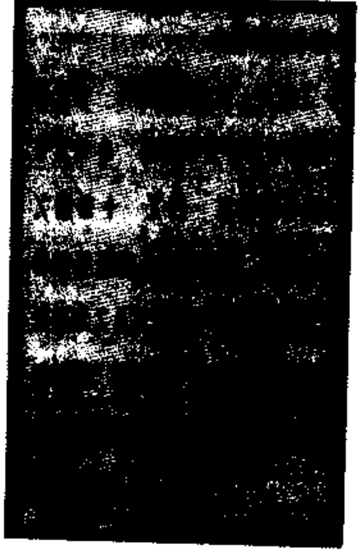
in der re.e. .aen.t man mit..en..i.an
der.e.t.att...erden a.er mit.e...i.
i.t die.e.t m.ede an.n..e..rden

现在我们有两个词,“.att”和“i.t”,缺少同一个字母。在密文中是两个 R。对于“.att”,我们在前面的尝试中就遇到过。“att”,当时被定为“satt”,同时还得到了“ist”这个词。和前面一样,我们把倒数第二个词定为“uns”,并由此得出,K 代表 u,于是倒数第四个词就可以破解了,即“muede”。还有两个单词只缺一个字母,即中间一行的“.erden a.er”。就这两个空位来说,T 很有可能是 W,I 则表示 b。“we.t”共出现了两次,到底是什么意思呢?我们试着选择“welt”。接下来看第三个单词“re.el”,推测它为“regel”,和上文一样。最后一个词现在只缺一个字母,我们用“geworden”来解释它,于是得到“…ist die welt muede an uns geworden”。实际上现在我们已达到了目的。

关于如何破译单码密文,并没有明白确凿的规则,但有用的规律的确存在,这要求脱密者具备敏锐的鉴别力和经验。

《法兰克福汇报》的弃儿

《法兰克福汇报》每周发行一份副刊。在它的猜谜角一栏中,以“弃儿”为题定期发表密文,由数学家及科技记者托马斯·冯·兰多采用单码撰写。与字母表上的字母相对应的符号一会儿用中国字,一会儿是乐谱,一会儿是古埃及象形文字。我们在前一章中处理的文章,就是从一篇“弃儿”中节选的。因为印刷技术方面的问题,我用字母代替了符号。图 5.9 和图 5.10 提供了更多的《法兰克福汇报》的“弃儿”。如果您有兴趣,不妨一试。这些例子相对而言较简单,因为单词间有间距相隔。在前面的分析中,我们就多次借助了对单词长度的确认。另外,这些文章都具有相当的篇幅,且使用日常用语。



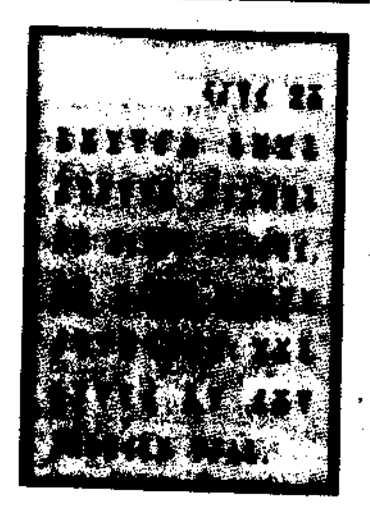
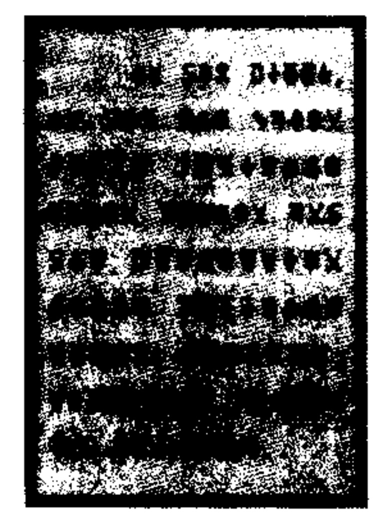
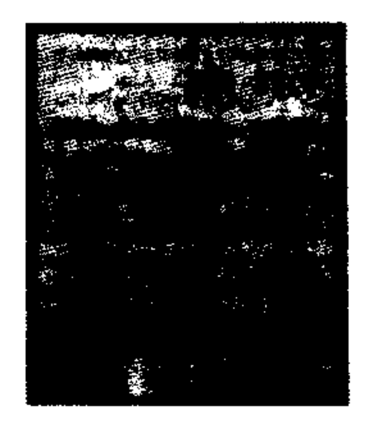
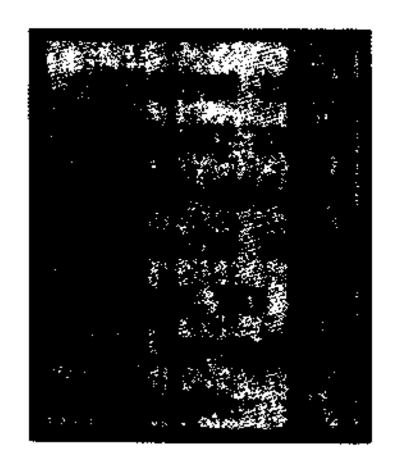


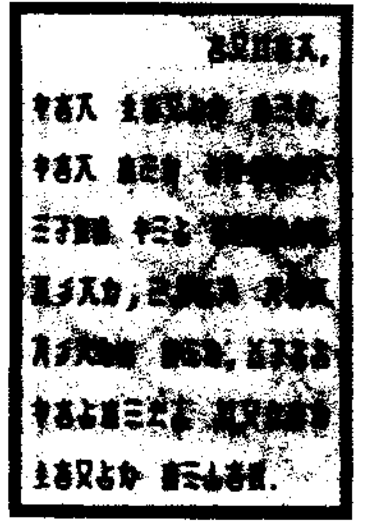


图 5.9 和图 5.10:刊登在《法兰克福汇报》副刊上的"弃儿"。









而在有些密文中，字母出现频率发生变化，事情就变得困难多了。数学家阿尔布雷希特·博伊特尔斯帕赫尔是密码学专家，他在专著《密码学》中引用了“Traktat ueber die amouroe-

sen aventueren des balthasar matzbach am rande des panamakanals"和"einfluss von ozon auf die zebras im zenfrum von zaire",作为伪造频率分布的例子。下面是一篇不设字间距的短篇密文,比起《法兰克福汇报》中的"弃儿"来,它的破解难度已有所增加。

KLEWMIHBILYEWGPLEWRHKGKEWJGEWGIL

我请诸位读者来解明文。破译成功者,将再得到一篇"弃儿"作为奖赏:

12234 5678 3A4 B36CD3E1B2F . 53AA 19HB AGHBF GJA
83A 232F3A , 83A3A 567 3F514 D3KJ7DF B1K3A

绦虫计

《法兰克福汇报》的每篇"弃儿"之前都有一段导言:"常用的字母和短词是打开成功大门的钥匙。如果加密者隐去文中的字间距和标点符号,那么呈现在读者面前的是一条状如绦虫的字母串,这时短词就失去了其作为辅助工具的意义。图 5.11 就是一个例子。这时,我们看不到短词的标志,因而只能求助于统计学,而在这种情况下,它会向我们透露一切。密文字母 N 出现次数最多,83 次,即 17.2%。其后是 F 占 12.0%,Q7.1%,E6.8%和 A6.4%。接下来的 3 个我们也作了统计,B6.0%,K5.8%,T5.0%。我们拿这个结果来对照德语中字母出现的频率情况,其中最常见的是 e,18.5%,和 n,11.5%。由此,似乎有理由将 N 及 F 同 e 及 n 对应起来。在图 5.12 中,这两个字母已被置换入绦虫式密文中。

现在我们来看第一行中的明文字母"ee.ne",那 Q 代表什

图 5.11:一篇不设字间距的密文

么呢? 它是密文中第三个最常见的符号,占 7.1%。根据频率分配表,Q 可能是 i、s、r、a 或 t 中的某一个。其中 i 最为契合,这也是因为 NQ 和 QN 两个字母对在密文中较常出现,它们应同明文中的"ei"和"ie"对应。于是我们假设,i 是正确的选择。我们试着把它放入文中,发现没有出现不对头的明文字母组合,恰恰相反,单词"eine"在明文倒数第六行中再次出现了。

我们把视线转向第一行的几个符号。我们已得到了".ie",那么第一个字母会是什么呢? 明文开头为"die","wie",还是"nie"? 最后一项可能性应该排除,因为 n 已用过了。在密文中,P 出现了 17 次,占 3.5%。德文中字母 d 使用率为 5.08%,而 W 则为 1.89%。推断其为 d 的可能性较大,

```
. . e . . . . . . . . . . . e e . n e . . . . . . . . . e n . e
. . . e . e . e . . . . . . . . e n . . . . . . e . . n n . .
. . e . e n . . . . . . . . . . . . e . e . e . . . n . . n .
e . . . n . . n . . . . . e . . . . . . . . . . . n . . . . . n
. . . . . . n . . e . e n . . . e n . . n . e n . n . . . .
. . . . e n e . e n . . . e . n . . . . n . . n . e . . n e
. . e . . . e . . . e n . e . . e n . . . . . e n n . . . .
. . . . e n . . . . e . e n . . e . e n . e . . . n . . e .
. . e . . n e . . n . e . n e . n . e n . . n . e n . . e .
. . . . . . . . . . . . . . . . . . . . . e . e . . . . . . n .
e n . n . . e n . . e . . e n . . . . . . . . . n . . . . . .
. e e . . . . e . . e n . . . e . n e . . . e . . e . . . n
n e n . e . . . . . . . e . . n . . . . . . e . . e n . n . .
e . . . . . e . . e . . . . . . . . . e n . . . . e . . . . . .
. . . . . e n . . . . . . . . . . . e . e . . e . . . . . . . e
. . . . . . . e . . e n . . . e n . e . . . . . . . . . . e .
e n
```

图 5.12:图 5.11 的密文借助频率分配破译的 e 和 n 两个字母推测出字母 i。

```
AANWTFNAQFENAFNYFLNFPBFZNFPQNK
..e..ne.in.e.ne.n.end.n.endie.
QWTYBWTYBBOBZAQRBKVNANWTEQZBFZ
i.............i....e.e...i..n.
NFBFPPNFJBNMMNFKWTBEOHXFKXRF
en.ndden..e..en.........n......
ANNAKEANWUNFCQENQFNARBN
.ee.....e..en.i.eine...e..e...n
```

图 5.13:图 5.11 密文中的一段帮助我们得到了字母 u。

但也不能排除 W。我们先用 W 来代替 P。如此一来,明文字母对“nw”在文中出现 10 次,颇引人注目。在常见的双字母组合中,以 n 开头的只有“ne”和“nd”。如此看来,“以 W 代 P”这一步很有可能将我们引入歧途。我们还是不妨尝试“以 d 代 P”,然后考察图 5.13 中的节选文章,其中第九至十二行中已知的明文字母已嵌入。在明文第三行可以找到“en.ndden”。由此推测,单词“und(和)”隐藏在里面。所以我们用 u 来代替 B,看看图 5.14 中的结果如何。u 看起来适得其所。第四行中的“indun.”引起了我们的注意。如果它是“indung”的话,那 Z 即 g。第九行也支持这一推断,这样就会出现“endung”。在此基础上再来看第三行中的字母串“.e.edeu.un”,我倾向于读作“Bedeutung”。如此一来,V 对应 b,E 对应 t,而 Z 则恰如我们所料,代表 g。我们来看图 5.15 中作了上述处理之后的第三至五行,单词“bedeutung”立即映入眼帘——我们的路是对的!紧接着是“in.e.bindung.it”,这当然只能解释为“in Verbindung mit”。至此,我们已用 V、r 和 m 分别置换了 H、A 和 C。如图 5.16 所示,可以看到由此得到的前两行密文。在结尾处可以看到“tge.innt”,其中很可能隐含着“gewinnt”,即 L 代表 W。我们看图 5.17,它反映了图 5.11 密文的第九至十一

```
PQNUADIEXMXZQNNQFNSYTAEYBKNEPN
d i e . . . . . . . . i e e i n e . . . . . . u . e n d e
YMENZNTNQCLQKKNFKWTYREZNLQFFEQ
. . . e . e . e i . . i . . e n . . . . . . . e . i n n . .
BKNTNFPKIAYUEQKWTNVNPNBEBFZQFH
u . e . e n d . . . . . . i . . . e . e d e u . u n . i n .
NAVQFPBFZCQEPNCKWTBEOHXFUXCCBF
e . . i n d u n . . i . d e . . . . u . . . . n . . . . u n
QUYEQXFKLNZNFPYENFVYFUNFBFPKXR
i . . . i . n . . e . e n d . . e n . . n . e n u n d . . .
ELYANFNVNFQTANAFBEOBFZQFANWTFN
. . . . e n e . e n i . . e . n u . . u n . i n . e . . n e
AZNKEBNEOENFXNRRNFEMQWTNFFYWTA
. . e . . u e . . . e n . e . . e n . . i . . e n n . . . .
QWTENFKDKENCNFEANENFCNTABFPCNT
i . . . e n . . . . e . e n . . e . e n . e . . u n d . e .
AANWTFNAQFENAFNYFLNFPBFZNFPQNK
. . e . . n e . i n . e . n e . n . e n d u n . e n d i e .
QWTYBWTYBROBZAQRRKVNANWTEQZBFZ
i . . . u . . . u . . u . . i . . . . e . e . . . i . u n .
NFBFPPNFJBNMMNFKWTBEOHXFKXRELY
e n u n d d e n . u e . . e n . . . u . . . . n . . . . . .
ANNAKEANWUNFCQENQFNARBNMMNKIYF
. e e . . . . e . . e n . i . e i n e . . u e . . e . . . n
FNFPNAMBKEQZNABFPVQKLNQMNFYFOB
n e n d e . . u . . i . e . u n d . i . . e i . e n . n . u
NZMQWTNAZNKWTQWTENFYBKPNATQKEX
e . . i . . e . . e . . . i . . . e n . u . d e . . i . . .
AQKWTNFUADIEXMXZQNZNLBNAOEQKEN
. i . . . e n . . . . . . . . . . i e . e . u e . . . i . . e
KYBWTRBNAPNFMYQNFANQOHXMMOBMNK
. . u . . . u e . d e n . . i e n . e i . . . . . . . u . e .
NF
e n
```

图 5.14:进一步脱密后的图 5.11 的密文。

行。在结尾处,"berechtigungen und"清晰可辨,那就是:以 C 代 W,h 代 T。在图 5.18 中,我们的明文已完成了相当一部分。

难道还需要我向诸位透露,接下来该怎么办吗?当然是将 Y、M、K、X、R、S、U、I 和 D 换成明文的 a、l、s、o、f、j、k、p 和 y。后者是从第八行得来的,通过 K 和 S 的互换,单词"systeme(系统)"跃然而出。最后提一句,这篇文章摘自一本著名的密码学论著的封底。

```
u . e . end . . . . . t i . . . e b e d e u t u n g i n .
e . b i n d u n g . i t d e . . . . u t . . . n . . . . u n
i . . t i . n . . e g e n d . t e n b . n . e n u n d . . .
```

图 5.15:图 5.11 密文中的一个片段,有助于破译字母 V,r 和 m。

```
d i e . r . . t . . . g i e e i n e . . . r t . u . e n d e
. . t e g e . e i m . i . . e n . . . . . t g e . i n n . .
```

图 5.16:借助图 5.11 的这部分密文,我们得到了字母 W。

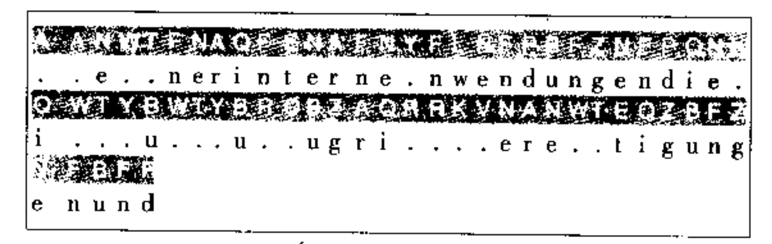


图 5.17:借助图 5.11 的这段密文,我们推断出字母 C 和 h。

[illegible]

die.r..t...gieeine..hrt.u.ende

[illegible]

..tegeheimwi..en.ch..tgewinntz

[illegible]

u.ehend..r..ti.chebedeutunginv

[illegible] EOHXFUXC [illegible]

erbindungmitdem.chutzv.n..mmun

OUY [illegible] FVYFUNFBFP [illegible] XR

i..ti.n.wegend.tenb.n.enund...

ELYAN [illegible] BEOBFZQFANWTFN

tw.renebenihrernutzunginrechne

AZNKEBNEOENFXNRBNFEMQWTNFFYWTA

rge.tuetzten.e..ent.ichenn.chr

QWTENFKDKENCNFEANENFCNTABFPCNT

ichten...tementretenmehrundmeh

AANWTFNAQFENARBYFLNFPBFZNFPQNK

rrechnerinterne.nwendungendie.

QWTYBWTYBROBZA [illegible] NANWTEQZBFZ

ich.uch.u.zugri...berechtigung

NFBFPPNFJBNMMNFKWTBEOHXFKXRELY

enundden.ue..en.chutzv.n...tw.

ANNAKEANWUNFCQENQFNARBNMMNKIYF

reer.tree.enmiteiner.ue..e...n

ENFPNXMBKEQZNABFPVQKLNQMNFYFOB

nender.u.tigerundbi.wei.en.nzu

NZMQWTNAZNKWTQWTENFYBKPNATQKEX

eg.icherge.chichten.u.derhi.t.

AQKWTNFUADIEXMXZQNZNLBNAOEQKEN

ri.chen.r..t...giegewuerzti.te

KYBWTRBNAPNFMYQNFANQOHXMMOBMNK

..uch.uerden..ienreizv...zu.e.

NF

en

图 5.18:图 5.11 中的密文已接近彻底脱密。剩下的部分很容易猜出。

扑朔迷离的频率

借助频率分析，事实上我们可以彻底破译任何一篇单码密文，只是它必须具备足够的篇幅。因此人们从很早就开始尝试，修改单码密文的规则。早在600年前，人们就发现了最简单的方法。从曼图亚的官方信件中，可以查到1401年的一种密钥。图5.19所示按此种规则进行作业的密钥，上面一行为明文字母表，下面是密文字母表，密文字母表含有字母和数字。对于明文字母e、i、n、r和s，加密者可以在数个对应密符中选择。这种方式使明文字母的自然频率分配变得扑朔迷离。“erdbeergelee”可以被加密成CB5YHQRXE3UC，这里e的多频性完全看不到了。

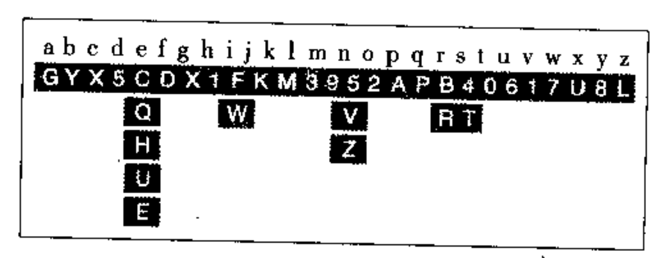


图5.19　对于明文字母表中的e、i、r和s，加密者可以在数个对应密符中选择。这样可以掩饰德语中个别字母的频率分配。

1401年的这种古老密钥告诉我们，曼图亚公爵办公室的书记员已远远超出了凯撒密表的水平，他们已知道了单码密文的致命弱点。今天我们已经掌握了任何一种语言中的字母频率分配。我们可以视不同情况，为每个明文字母配备数量合适的密符，以便使密符在一篇较长文章中的出现频率大体相同。例如，我们可以把00，01，02，……，98，99配备给德文

字母表中的26个字母。对于不同的明文字母，如b和f可以各配两个，而c，g，l，m，o和u各三个，h应有四个密符，而a和d，我们分给它们各五个，t总共给六个，r和s各七个，i可得到八个，n甚至达到十个，最后我们替e准备了十七个密符。其他的字母只对应一个。这样，每个字母都拥有了自己单独的密码表，它掩盖了德语中的字母频率分配。因而，即使e是出现频率最高的字母，但由于它拥有十七种不同的符号，在密文中就不那么容易被发现了。

这种所谓的"同音"加密的一个弱点在于，收发双方都无法将密钥默记于心。他们走到哪儿，就得把它带到哪儿，每次双方都需要事先交换密钥。从另一方面说，这种方式也远未达到理想的可靠性。虽然e的"庐山真面目"难以辨认，但在任何一个语种里，一些字母组合的使用总是比另一些更为频繁。只要密文达到一定篇幅，我们就可以考察哪些符号组频繁出现。也就是说，破译者面对一篇"同音的"密文不可能完全束手无策。

还有一种情况，如图5.20所示的正方图形，也会导致字母出现的典型频率模糊难辨。对于出现频繁的字母，加密者可以在这儿使用一种方法，在那儿用另一种他注意到的方法。例如e可能是02或76，但也可能是61。这样一来，其频率就被掩盖起来了。例如，"leberwerte"可能会被编为55106227833405875461。这时，频率分析对于解密者也毫无帮助。

尽管如此，密码学家还是会察觉到，整篇密信由偶数位的数值组成，即每个字母都由一个数字对来表示。由此推断，字母嵌在一个十横行十纵列的正方形中，分别对应0、1……9。然而他还远未达到目的，因为他还不清楚，字母是以怎样的顺

序填入正方形的空格中。当然在相当篇幅的文章中，诸如"ch"之类的高频率字母组合，其相应的数字对组合很容易引起注意。

	0	1	2	3	4	5	6	7	8	9
0	n	h	e	d	n	e	r	o	i	e
1	e	m	c	s	o	e	b	s	g	n
2	t	r	a	e	t	h	i	e	s	t
3	a	e	g	d	w	r	n	d	n	v
4	i	u	i	k	e	d	c	z	m	s
5	n	s	d	n	t	l	j	l	q	n
6	r	e	b	p	i	n	o	l	i	u
7	e	g	s	e	h	y	e	f	s	a
8	i	n	f	r	u	r	x	r	a	h
9	t	e	c	m	a	e	e	t	e	i

图 5.20：一份可以掩盖德语字母正常频率的密钥表，每一个明文字母对应一个数字对，比如 58 是 q，77 是 f。对于经常使用的字母，则有多个数字对可供选择，如 e 可以选择 02、05、09 等中的一个。

图 5.20 只是一种可行的密钥表的一个例子。人们随时可以再编一份密钥表，其中字母表中的字母以同样的频率出现，但顺序却不一样。

世界上最重要的秘闻之一，正是通过这种方式加密的。第二次世界大战中，美国核弹项目负责人莱斯利·理查德·格罗夫斯将军，在电话中用数列来代替一些重要的词语，他正是读了类似图 5.20 的密钥表。

还有另外一种方法，可以用来阻碍破译者进行频率分析，我们会在下一章中了解它。

不公平的"公平游戏"

如果您和您的情人通信，并使用双方约好的名为"普莱费

尔"的加密方式,那么对您的配偶来说,这不是什么公平游戏。不过,事实上这名字本身也不正确。普莱费尔(英语意义为"公平游戏")·冯·圣·安德鲁斯男爵是英国维多利亚时期的社会名流,他担任下院发言人和英国科学促进会主席。他大力推行英国卫生事业的改革,物理学家查理·惠斯通是他的挚友。由于惠斯通电桥的命名,他的名字在电学中至今为人所熟知。

两个人选择了共同的业余爱好:密码学。当时伦敦的《泰晤士报》经常刊登加密的私人通告。两人以破译这类密信为一大乐事。他们也正是以这种方式,追踪一个牛津大学生和伦敦一位女士的书信往来,这位女士显然已嫁为人妇。当年轻人怂恿这位夫人同他私奔时,惠斯通在《泰晤士报》上用情人的密码刊登了一封信,信中规劝这位女士迷途知返。随后登出一行简短的密文:"查理,别再写信了,我们的密码已被识破。"

惠斯通本可以向他们推荐一种更好的加密方法,这是他自己发明的。后来他的好友普莱费尔将其发表,他并没有隐瞒原发明者的名字,然而直到今天,这种密码依然被称为普莱费尔(公平游戏)。它的着眼点是将字母"对"加密,而不是字母。

这种加密方法根据下列规则才能生效:先编制一张密钥表,当然它最好是自己独立思考的产物。接下来与"带提示词的凯撒密表"相似,选取一个提示词,隐去叠双字母,然后附上字母表中的剩余字母。i 和 j 等同视之,于是字母表由 25 个字母组成。它是一个正方形,有 5 个横行,5 个纵列。密钥词 ORCHIDE 从属于提示词 Orchidee(兰科)。在此基础上建立图 5.21 中的正方形。

O	R	C	H	I
D	E	A	B	F
G	K	L	M	N
P	Q	S	T	U
V	W	X	Y	Z

图 5.21：一张 5 横行 5 纵列的密钥表，其中字母表的 25 个字母顺序是借助提示词“Orchidee”确定的。

我们以下列明文为例

ichkommeammittwoch

我们将其分解成对：

ic hk om me am mi tt wo ch

如果我们在密钥表中查找一个字母对，可能出现下列 3 种情况：

1. 两个字母处于同一横行。
2. 两个字母处于同一纵列。
3. 两个字母既不在同一行，也不在同一列。

具体情况，具体对待。

情况 1：我们将横行中紧随其后的两个字母代替明文字母来进行加密：OC 变成 RH，对于诸如 fe 这类字母对，我们必须改变作法，因为 f 无后继字母。在这种情况下，我们选用这一行的第一个字母，于是 fe 变成 DA。以此类推，SU 现在为 TP，nm 为 GN。

情况 2：如果一对中的两个字母处于同一纵列，那么应由它们下面的两个字母代替，从 sa 可得到 XL。对于其下无后继者的字母，则采用这一纵列的第一个字母。zn 变为 IU。

情况 3：我们从一对中的第一个明文字母开始，向左或向右，进至第二个明文字母的纵列。处于相交位置的字母，作为

密文对的第一个字母。再从明文对的第二个字母开始，水平到达第一个字母的纵列。于是 om 变为 HG，mo 为 GH。

当字母对由两个相同字母组成，如将明文单词"Mittwoch"分解成字母对"mi tt wo ch"，则必须进行特殊处理。我们对 tt 怎样处理呢？规则是：改变明文，避免这种情况发生。比如，我们可以把"mittwoch"分解成"mi tx tw oc hx"，熟练的脱密者会从中辨认出"mittwoch"。

这种密码看上去很难，但熟能生巧。图 5.22 列出了字母对对应的多种情况。

下面是明文和对应的密文：

ic hk om me am mi tx tw oc hx
CH RM HG KB BL NH SY QY RH CY

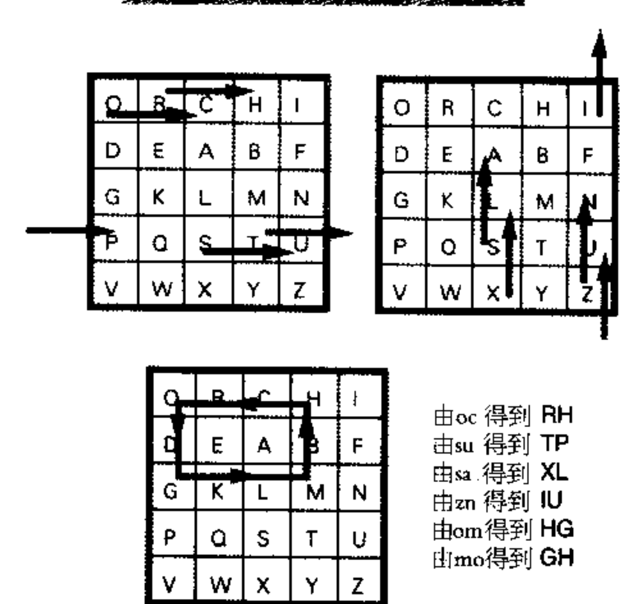


图 5.22：运用公平游戏—正方形加密，"Orchidee"被选作提示词。细节请参见文中解释。

在破译密码时，我们反其道而行之。在第一、二种情况下，我们选取其前和其上的字母，如遇到处于横行或纵列第一个字母，则取最后一个字母。对于第三种情况，我们的作法同加密时毫无二致。

在公平游戏一密码文中，常见的字母不再那么醒目，经常出现的字母对还会引人注意。但是它们的频率分配比单个字母更平均。即便如此，如果供我们使用的密文具有相当的篇幅，这种加密方法同样可以被破译。

第二次世界大战中的公平游戏

如果我们改进公平游戏的规则，即在此基础上重复使用一次，那么，破译者的日子就更难过了。我们按任意顺序两次将字母填入不同的5行5列正方形，并仍然将 i 和 j 视为同一个字母。图 5.23 是一份由两个正方形组成的密钥表，每个正

i	k	p	u	d	a	l	q	y	f
l	a	m	e	r	k	z	h	g	t
x	c	t	s	o	u	r	c	s	m
h	n	b	g	w	p	d	i	n	x
f	v	z	q	y	v	e	o	w	b

图 5.23：第二次世界大战中使用的双柜加密法。它的加密单位不是单个字母，而是将明文字母对转换为密文字母对。

方形内有 25 个字母。在第二次世界大战中德国人称其为“双柜”。为便于加密，我们将明文分成相同长度的行，并保证行数为偶数。如果需要，我们可以在最后一行填入任意的字母。这种方法不是以单个字母，而是以上下列的字母对为单位，进

行加密。例如明文为：

w i r k o m m e n
m o r g e n x x x

我们从字母对 w/m 入手，从左边正方形的 w 至右边的 m 划一个箭头。（图 5.24）接着再绘出这条直线的对角线（图中为灰色）；它是由右边的 x 到左边的 o。这是加密的第一步：由 w/m 得到 x/o。在此基础上，我们在左边的正方形中再重复一次，由左边的 x 到右边的 o 划一个箭头，同样作水平反射，这样，我们就有了一个新的箭头，从右边的 c 指向左边的 f：x/o 变为密文字母对 **C/F**。总的来说，经过两次加密后，字母对 w/m 转换为 **C/F**。对于第二个字母对 i/o，我们也进行同样处理：箭头由左边的 i 指向右边的 o，经水平反射得到 q/f，然后从

i	k	p	u	d	a	l	q	y	f
l	a	m	e	r	k	z	h	g	t
x	c	t	s	o	u	r	c	s	m
h	n	b	g	w	p	d	i	n	x
f	v	z	q	y	v	e	o	w	b

i	k	p	u	d	a	l	q	y	f
l	a	m	e	r	k	z	h	g	t
x	c	t	s	o	u	r	c	s	m
h	n	b	g	w	p	d	i	n	x
f	v	z	q	y	v	e	o	w	b

图 5.24：采用“双柜”方式进行双重加密。上图中的箭头对应字母对 W/m，由左边的 w 斜至右边的 m，对这条斜线作水平反射，得到一条由 x 至 o 的灰色线。于是通过第一步，明文字母对 w/m 转换为密文字母对 x/o。现在我们将 x/o 作为新的明文，也就是说，对 x/o 进行同样的加密处理（见下图）。结果得到了由 C 划至 f 的灰色箭头。于是 w/m 在第二步中转换为密文字母对 C/F。

左边的 q 至右边的 f 划一箭头，通过反射得到 B/U，于是密文以这两行开头

我们可依此类推下去。但事情并不总是这么简单，需要加密的字母对有可能位于两个正方形的同一行中，这样一来，它们的连线无法作水平反射。例如最后一个字母对 n/x 就属于此类情况。连接箭头被水平反射后，得到 X/N，经过两次加密，我们又看到了原来的字母对 n/x。为避免这种情况发生，有必要强调一条特殊规则，因为对它的描写可能会太长，所以我把它用框形锁定。

> 对于一条水平向右的箭头，首先要作水平反射，然后向左移动一个字母的位置。如要为 n/x 加密，那么用反射及推移后的箭头连接右边的 n 和左边的 h。于是第一次加密使 n/x 变为 n/h。左边的 n 和右边的 h 组成的这条斜线，在反射后得到 i/a。假设我们要将 x/r 加密，不过到目前为止还存在一个困难。连接左边的 x 和右边的 r 的箭头是水平的，把反射后的箭头向左推移一个字母的位置，它就会越过左边正方形的边线。在这种情况下，应取右边正方框最后纵列中的相应字母，即 m。于是在第一次加密后，x/s 转换成 u/m，然后由 u/m 最终成为 F/S。

脱密的过程相应如下：对于密文字母对 C/F，我们从右边的 c 划一箭头至左边的 f，经水平反射得到 x/o，再次反射后，由右边 x 至左边 o 的箭头变为 w/m，即原来的明文字母对。

我们依然可以通过两个提示词来确定两个方形内的排序。类似于《带提示词的"凯撒密表"》中所讲到的，隐去提示

词中的字母重复部分，并将其作为密钥词逐个字母地写入正方形空框的前几格，然后再填入字母表的剩余部分。如图 5.25 所示，就是一个"双柜"，它的提示词是"Tageszeitung"和"Orchidee"，由此得到相应的密钥词为 TAGESZIUN 和 ORCHIDE：

t	a	g	e	s	o	r	c	h	i
z	i	u	n	b	d	e	a	b	f
c	d	f	h	k	g	k	l	m	n
l	m	o	p	q	p	q	s	t	u
r	v	w	x	y	v	w	x	y	z

图 5.25：一个根据提示词"Tageszeitung"和"Orchidee"构造的"双柜"。

在第二次世界大战中，德国保安机关、党卫军和德国国防军均使用过"双柜"。密钥表每 3 个小时就会变换一次。为了表示隐去的 j，写成 ii，于是"jagdflieger"就变成"iiagdflieger"。就连这种复杂的公平游戏的文本，英国的保密机构也可以解读。[1]

如果我们把数字引入密钥表，双柜加密法就更复杂了。例如，我们取 I 和 J 作为两个密符，并起用 0 至 9 这 10 个数字，那就可以构造出一个 6×6 个密符格的正方形数字密钥表。

---

① 弗里德里希·L·鲍尔：《破译的秘密》，海德堡/柏林，1995 年，第 56 页。J·S·施利克，"1942—1945 年与秘密情报处 849 室在一起"，《密码学》，1987 年 1 月，第 29 页。

1 1

8

6

排列整齐的“凯撒密表”

布莱兹·德维吉尼亚于 1523 年 4 月 5 日出生在圣—珀尔塞。他大学毕业后在不同的主人处从事外交事务。1570 年，他在 47 岁时，放弃公职，致力于写作。他的《密码论》于 1585 年出版。这本 100 多页的论著还包含了许多密码学以外的知识——日本汉字、炼丹术、巫术、犹太神秘教义、炼金术，但文中也真实而详尽地反映了那个时代的密码学水平。

弗里德利希·L·鲍尔《破译的秘密》

单码字母相对而言易于破解。因而在文艺复兴时期，人们就开始尝试同时将多个字母转换为密码形式。

不完全被人相信的修道院院长

15 世纪的德国学者约翰内斯·特里特缪斯(1462—1516)，以

创作多部传记而闻名。他出生于摩泽尔河畔特利滕海姆的一个葡萄园主家庭，其时正是莱奥纳多·达·芬奇的后十年和发现美洲大陆前三十年。20 岁时，他进入施蓬海姆修道院，两年后成了修道院院长。他的兴趣广及炼丹术，星占学和各类神秘学科，这也符合当时的潮流。据说他还认识真正的浮士德博士，这位歌德笔下的浮士德的原型，在他的眼中是个江湖骗子。其实他自己也算得上一个。在研究中他发现，巫婆分为 4 种不同的类型；历史是以 354 年为一个周期；创世在耶稣诞生前 5206 年就已完成。他声称自己知道如何通过天使，向另外一个人传递消息，这称得上是文艺复兴时期的 e - mail。此类牛皮使他无论在教堂，还是在修道院僧侣中，都声名狼藉。他不得不离开施蓬海姆，被维尔茨堡的一个修道院收留，不久就晋升为院长。他在那儿写了 6 本关于密码学的著作，对每本书，他声称自己只用 10 天时间。他在 54 岁时逝于维尔茨堡，他的著作也稍后在那儿出版。其中最重要的一篇论文见于第五本书，这时正方形密表首次问世。图 6.1 中可以看到它稍加改动后的形式。

密表如何形成不难理解。第一行为明文字母表，矩形表格中的第一行重复第一行，第二行则把第一个字母放到最后一位，接下去再把第二行的第一个字母后移，以此类推，一行的第一个字母总是出现在下一行的末尾。在单码加密中，一个密文字母正好对应一个明文字母，而现在可以用 26 个密文字母来对应一个明文字母。

假设我们要为明文"sendet bitte hilfe"加密。按照特里特缪斯规则，加密步骤如下：对明文的第一个字母，应参照密表的第一行加密，这样 S 变为 S，这并不费劲，但事情的进展不会一直这样简单。第二个字母根据第二行加密，于是 e 转换为 F。而第三个字母 n，转成第三行中的 P。接下来的步骤

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

图 6.1:特里特缪斯密表。在方形中,逐行向左推移一个字母,然后把左边多出的那个字母填入右边的空位。表格上方为明文字母表。加密时,对于明文第一个字母使用第一行的字母表,事实上没有发生变化。而加密第二个字母时,则使用第二行字母表,第三个字母对应第三行,以此类推。这张密表也适用于维吉尼亚加密法。这种加密法有一个密钥词,其字母表示用哪一行来为哪个明文字母加密。譬如密钥词为 HUND,明文字母将按顺序分别利用以 H、U、N 和 D 开始的那几行加密。接下来依然利用密钥词周而复始地进行下去。

一目了然：d 变为 G，e 这次为 I，t 为 Y。最后得到第一个单词的密文 SFPGIY，整条密文是 SFPGIY HPBCO SUYTT。如果明文超过了 26 个字母，可以周而复始进行，也就是说，加密第 27 个字母时，我们又回到了密表第一行的字母表。

其实这并不是什么新鲜事物。密表中各行是简单的凯撒推移表。但现在两者的根本不同之处在于，不再使用同一份凯撒密表对整篇文章加密，而是每个字母各对应一份不同的凯撒密表。为体现这种加密方式与单一字母表的区别，人们将它称为“多字母替换法”。明文中有 4 个 e，每一个都转换成不同的密码字母，这样泄密的字母出现频率就被掩起来。一旦有人知道了加密程序，就可以破译密文，他可以循规蹈矩地按顺序将每一行制成密表，也就是用第十七行的字母表来为第 17 个字母脱密。特里特缪斯体系的长处在于，在重复使用第一行字母表加密之前，已使用过 25 份凯撒推移表。

在此基础上，只需一小步，就可以突破这个呆板的老框架，即“第一个字母——第一行字母表，第二个字母——第二行字母表……”。很快，文艺复兴时期的几位人士就跨出了这一步。其中包括跨学科的天才乔瓦尼·巴蒂斯塔·德拉·波尔塔(1535—1615)，他精通自然科学，可同时又醉心于巫术和戏法。这个伽利略的同时代人，20 卷《大自然的魔法》的作者甚至认为，可以用一块磁石来检验女性的童贞，他还透露，用什么样的魔术可诱使妇女宽衣。德拉·波尔塔也为密码学作出了重要贡献。同样，意大利数学家、医生及哲学家吉罗尼莫·卡尔达诺(1501—1576)的论著也不仅涉及数学、天文学和星相学，还涉及到上帝和世界。他还探讨了国际象棋和博弈、毒剂、梦、尿、牙齿和智慧。他的著作中有两本致力于密码学。看起来，当时投身于这一学科的人，涉及到三教九流的各式人

物。在这方面，布莱兹·德维吉尼亚(1523—1596)也不例外。他早年即成为一名外交家，为内韦尔公爵工作，他几乎整个一生都恪守此职。在罗马，他同教皇的密码学家们过从甚密。他钻研特里特缪斯、卡尔达诺和德拉·波尔塔的著作，并创立了不少加密体系，这些体系完全不拘泥于凯撒密表。他的成果在其身后被完全遗忘，直至19世纪，人们才重新对他表示关注。

布莱兹·德维吉尼亚密表

今天，维吉尼亚的名字与一个非常简单的密码体系联在一起。这个体系比特里特缪斯更进了一步，但还是建立在图6.1的表格基础上。如果我们避开"下一个字母——下一行"的套路，解密立刻变成困难重重。我们甚至根本不需要使用表格的所有行。比如我们可以按顺序使用第七、一、三、六、十和二十五行为前6个字母加密。如果信息长于6个字母，我们再从头开始，即回到表中第七行。"sendet"被转换成"YEPINR"，接收者只有在知道使用7,1,3,6,10和25数序的情况下，才能破译密信。这个数序得作为密文通过另一途径告诉他。

至此，我们可以发现程序(算法)和密钥之间的明显区别，密钥即7、1、3、6、10、25这一数序，而程序则隐藏在可以随时重构的密表中。密钥必须牢记在心。为了确定行列顺序，可以考虑一个特定的日期，如婚期，或电话号码，当然不能带零。我们也可以不以数字定序，而选择一个便于记忆的密钥词来确定行序。假设密钥词为KATZE，那么明文"sendet bitte hilfe"中的第一个字母，就要根据以K开头的那一行来加密：S变为C。负责第二个字母的是A－行，——e还是E——，对应第三个字母的是T－行：n变为G，以此类推。到第六个字

母,我们又从头使用 KATZE。最终明文变为 CEGCID BBSXO HBKJO。

为简化加密工作,我们将密钥词的循环形式写成一行,下面对应明文,如图 6.2 上部所示。然后我们可以按图索骥,在密表中寻找对应的密码字母,写在下面。图下半部分则展示了应如何解密。我们还可以撇开密表,而改用图 4.2 中的密码轮。在用密钥词 KATZE 来为第一个字母加密时,我们这样调节密码轮,使明文字母 a,即外圈的 a 同内圆的密码字母 K 叠合。通过这种调节,文章中的第一个字母被加密,S 变为 C。以此类推下去。



图 6.2,上:用维吉尼亚密表和密钥词 KATZE 加密;下:相应的解密过程。

维吉尼亚密表的运算程序,并不是秘密。但密钥词应由收发双方共同约定。而且一定要保密。

模糊的频率

多字母替换法可以使一种语言中的典型性字母频率模糊不清,特别是当我们选择字母尽量少重复的密钥词时。如果有人选 BBBBB 作为密钥词,即使根据维吉尼亚密表也会得到

一份单码密文,而且是简单的凯撒密码。

接下来我们研究一篇 342 个字母的明文,我已将其按维吉尼亚式程序加密。我先不透露明文。我们在破译中自然会得到它。当然我也不会把密钥词告诉你们,不过你们应该知道,它是由 4 个不同的字母组成的。关于明文中单个字母的出现频率,我只能透露下列信息:它们同图 5.3 中的字母相当吻合。字母 e、r、n、i 和 t 在明文中使用频率分别为 17.0%、8.5%、7.9%和 7.0%,而 v 只有 0.6%,j 更是区区 0.3%。字母 q、y 和 z 在明文中根本没露面。

密文请见图 6.3。为达到一目了然的效果,我将其按 5 个一组分列。最常见的字母为 9.1%的 L。由此可见,这不是单码加密,否则同 e 相对应的密码字母应以大约 17%的频率出现。最少出现的密码字母是 S(0.6%)。通过加密,文章中字

```
HFOUL WUWIY HWLFF SHWUH YCFWP
GUDBJ GELLH ILCAG BLPKH OFVLL
VRLMR UDCFV LHFFO USWSY EGLLZ
DABRP HHVNL LNQKY EMBMG XZFVH
ICTXU CIHYM VWHYG DYVRL AYGDB
WUQLV RQIYE XMFVF OHVFO NNOZA
RKLCZ FVXRH EJRUA YOHPG OXUXR
VUUPK YCPKA YAGPY AVAXB FOAVO
AMRLU CAWLL RVZYI RYUYO LGQHY
YEIVL FFOOA JBHQH UNJLJ EYXUA
FRNYA DUHGH YWULW ENUAY AXUXQ
HYZED NYJLL MVFOY EGHLN XMARV
WYVFO YEWLC AIVLZ DACBQ LHTHT
UPKAQ RUKYA NVYAQ LH
```

图 6.3:一篇采用 4 字母密钥词,并根据维吉尼亚密表加密的 5 字母一组的密文。

母的频率差别被掩盖了。如果说明文中的字母频率范围在0—17%之间，那么密文中就是0.6—9.1%。最高频率降低了，而最低频率则提高了。

如果我用一个由10个不同字母组成的密钥词来加密这一篇明文，这种趋势就更明显了。图6.4中展现的就是这样一篇密文。V拥有最高频率7.9%，最少的依然是B，1.2%。于是我们得到一条规律：密钥词越长，密文中的单个字母频率分配就愈趋于平均。

```
SNICE YPGFV MVLWS XIPLV JKZEI
IPNYG LDLCU BMVRU MTJSA QAFII
AQLDE NEVWJ WPZNH WNGPV JFLCM
WBUID SVPVE NIAHV JLBDT QAYMV
TKNFN EDRVJ AVHPT WZOIZ LGALU
YPAIS WPIPR QNYMT ZPPNH PIYWX
WJLTM YWQIV PRLCT AJRMD TWUOE
OVNGY JKJST AVQMV FUAOO YPTMC
LULTN EVGII WUZPV KZNPC WOKPR
AZSSI KEOFN CCAHV FVOTC GTHRX
KQNPN WVAXV JEOTP GIEXV FWUOD
AZSVR YGDTE OQPLV JFHCA QNTIJ
HGPNH AZGIZ FHVCM WBVSE WPNPM
WKUXN WTKPN GWRRE WP
```

图6.4：一篇采用10字母的密钥词，按照维吉尼亚密码得到的密文。其明文同图6.3中的一样。

木锤破译法

人们应该相信，维吉尼亚密文在电脑时代容易对付。归根结底，人们只需推测出密钥词。密钥词由字母表中的字母

构成，而一份字母表有26个字母。人们可以把计算机当成一个庞大的密钥词库，利用它来逐个检验可能的密钥词。

我们可以认为，没有人会使用一个或两个字母的密钥词。用单字母密钥词产生的是一篇单码密文，而双字母密钥词提供给我们的同样是一篇易被破译的密文。我们再试一下3个字母的密钥词。从26个字母中任意选3个字母，会有多少种组合形式？数学家们提供了一个简单的公式：26×26×26个组合方式，即17576个。通过这17576个密钥词，我的计算机提供了17576种明文。如果密钥词真的只有3个字母，那么这些文章中会有一篇是合乎情理的，在浏览时会引起我的注意。但我不必把它们全都读一遍，我可以教给计算机，在一篇正常的德语文章中，有一个字母大概以17%的概率出现，其次为11%。如果它只提供符合频率特征的文章，我的工作量就大大减小了。我还可以教给电脑其他的德语细节，如ch，sch，en和ne的频率之类，这也会减轻我的工作。

密钥词越长，使用这种木锤法破译就越困难。如果我在3字母密钥词处没有找到答案，那我就要求助于4字母密钥词，此类组合有26×26×26×26个，已超过450000个。要是这次我还是一无所获，那就必须根据5字母密钥词继续寻找，这样的词将近1200万个。倘若这样还是没有找到一篇有意义的文章，于是密钥词的长度达到了6个，这次我必须尝试3.09亿种情况。面对成亿的文章，即使我和我的计算机看一篇只需一秒钟，以确定它是否合适，那我们也得日以继夜地工作近10年。密钥词越长，工作也拖得越久。类似Donaudampfschifffahrtsgesellschaftskapitänswitwe（多瑙河汽船航行协会主席遗孀）这个密钥词，由47个字母组成，要检验所有可能的密钥词，我和计算机需要连续工作的年数达到了60位。

而天文学家估算宇宙的年龄,也不过10位数。

在一些加密方法后经常附注着,要得到最后的答案,需要检验多少种情况。这大多指用木锤方法。在第二次世界大战中,德国认为"恩尼格玛"机提供的加密方法是不可破译的。要想得到明文,需要一一尝试的方法数目惊人,德国人以为这足以保证加密的安全性。然而,他们犯了可怕的错误。即使破译简单的维吉尼亚密码,人们也必须对所有的密钥词进行检验。早在人们预测到计算机出现之前,一位东普鲁士军官就发现了这一点。

如何破译维吉尼亚密码

一眼望去,人们几乎无法从维吉尼亚密文中读出什么有意义的东西。事实上,在很长一段时间内,维吉尼亚加密法都被认为是安全可靠的。

从根本上说,您现在已得到了破译图6.3和6.4两篇密文所需的所有信息。您根本不需要密钥词,起决定作用的是它的长度,这我已透露给您了。

现在我们来看图6.3中的密文。因为密钥词的长度是四位,所以第一、五、九、十三……个字母是用密钥词的第一个字母加密的,对于2、6、10、14……等字母使用的则是密钥词的第二个字母。这也适用于3、7、11、15……及4、8、12、16字母。我们从124页的文章中挑出用同一个密钥字母加密的那些密码字母。如图6.5所示,我们得到了4组密文字母。

不知你是否注意到了,我们已接近破译这篇密文。这4组字母中的每一组分别是用同一个凯撒密表加密的。一组相应的明文字母,使用的是密钥词的同一个字母,即维吉尼亚表

中的同一行，每一行对应一个凯撒密表。

德语明文中随便哪个字母，都应具有德文中的典型性频率，如 e 很有可能以 17% 的频率出现，结果必然是，代表 e 的密码字母出现特别频繁。我们先来看用密钥词第一个字母加密的那组字母：L 最常出现(19.8%)，然后是 A(10.5%)，紧接着 U 和 Y(各 9.3%)。L 极有可能代表 e。我们再回过头去查阅图 6.1 中的维吉尼亚表，看在哪一行中 e 以 L 置换。原来是第八行——此行以 H 开头——由此可推测，我们面对的是历经 7 次推移后的凯撒密表。事实上，根据图表的这一行，密文字母组中出现最多的字母之一 U，也对应了德语中第二位最常出现的字母 n。假设第一组密文字母是用 H 行来加密的，我们就得到了相应的明文字母。这样，密文中四分之一的字母已脱密，而且，我们还赢得了密钥词的第一个字母，H。

Mit dem ersten Schlüsselbuchstaben wurden chiffriert:
HLILHYPBLLBHLLDLOSLAHLKBZIUYHYABLIMOOZLVEAPUUYAP
AOAULZYLYVOBUJUNUYWAUYNLOHMWOLVALTAKVL

Mit dem zweiten Schlüsselbuchstaben wurden chiffriert:
FWYFWCGJLCLOLMCHUYLBNLYMFCCMYVYWVYFHNACXJYGXU
CYYXAMCLYUGYLOHNEAYHWEYXZYMYLAYYCLCHUQYYH

Mit dem dritten Schlüsselbuchstaben wurden chiffriert:
OUHFUFUGHAPFVRFFSEZRVNEGVTIVGRGUREVVNRZRROORPP
AABVRARIYQEFAQJYFAGUNAQEJVENRVEAZBTPRAA

Mit dem vierten Schlüsselbuchstaben wurden chiffriert:
UWWSHWDEIGKVRUVFWGDPNQMXHXHWDLDQQXFFQKFHUH
XVKKGVFOLWVROHIFJHLXRDHLUXHDLFGXVFWIDQHKUNQ

图 6.5：图 6.3 中维吉尼亚式加密的密钥词长度为四位，利用这一认识能把密文字母组成字母组，它们由密钥词的同一个字母置换。

相同的作法适用于另外3组密文字母。简而言之,按行序,最常出现的字母分别为Y(22.1%),R(14.1%)和H(11.8%)。如果3个密文字母都与明文字母e有关,那么3组密文字母分别是用U,N和D行来加密的,也就是说,密钥词是HUND(狗)。我们依次使用维吉尼亚密表中的H,U,N,D,H,U,N和D行,来破译密文开始的字母HFOULWUW……。如果我们继续进行下去,密文就变成:

albrechtbeutelspacheristimhauptberufeindurchausserioeserwissen
schaftlerdermathematikeranderjustusliebiguniversitaetarbeitet
auchnebenberuflichnichtalsgeheimcodeexpertebeimbundesnach
richtendienstdochgiltseininteressevorallemdererforschungund
entwicklungsogenannterchipkartenundderfragewiesicherdarauf
gespeicherteinformationengemachtwerdenkoennen

这篇文章摘选自1995年2月15日的《法兰克福评论报》,当然我去除了其中的标点符号。

对密钥词的长度的认识足以帮助我们把一篇维吉尼亚密码转换成几篇易解的凯撒密码。不过您可别忘了,这是我告诉您的。如果没有我的帮助,您将面对一项更为艰巨的任务。那么怎样才能得到密钥词的长度呢?

密钥词的节律

如果我们有一篇根据维吉尼亚密表加密的密文,但对密钥词长度或密钥本身一无所知,是不是就一定毫无办法对付呢?不是的,在用HUND加密的例子中,我们可以看到由其长度造成的节律,也反映在密文中,即每隔3个字母,由同一个

凯撒密表加密。戴维·卡恩在其关于密码学的经典著作[①] 中写到:"这种反复泄露密文中表层之下密钥词的举动,就像钓竿上的浮标告诉我们,鱼儿何时咬钩了。"

在维吉尼亚密码诞生后一个世纪,东普鲁士第三十三步兵团的一位军官作了一篇怎样确定密钥长度的论述。弗里德里希·W·卡西斯基(1805—1881)出生于西普鲁士的施洛豪。他在 17 岁时人伍,并在短时间内升为军官。后来他以团级少校退伍,终于有足够的时间致力于密码学。1863 年,他的著作《密码与破译术》在柏林出版。这本书只有 95 页,当时几乎未引起什么反响。不久,他放弃了密码学,成为一名业余人类学家。他发掘史前墓穴,并在专业刊物上作有关报道。他可能从未意识到,自己对密码学进行了革命,让我们来追循他的思路。

在德语中,有些字母使用特别频繁,如 ch 或 cht。而在维吉尼亚密码中,它们大多被转换成不同形式的密文字母组合。在原文 150 页中,单词"der"出现了 4 次,它一次被加密为 GLL,还有一次是 KYE,而另外两次是 QHY。其相应的密钥字母第一次为 DHU,第二次 HUN,后两次则是 NDH。对于前两种情况,我们用不着惊奇,因为"der"是用密钥词的不同部分加密的。而最后两个"der"正好相反:它们恰巧碰上了密钥词的同一部分,即 NDH。只有当密文中两个相同字母组之间相隔的距离恰好是密钥词长度的倍数,才会出现这种情况。这可以从图 6.6 中看出来。图中反映了图 6.3 第九至十二行的密文及相应的多次重复使用的密钥词。两者所强调的相同的 3 字母组合 QHY 分别由密钥字母 NDH 加密。两个 Q 间的

① 《破译者》,纽约,1967 年,第 208 页。

距离有 52 个字母,正好是密钥词长度的 13 倍。

HUNDH	*UNDHU*	*NDHUN*	*DHUND*	*HUNDH*
AMRLU	CAWLL	RVZYI	RYUYO	LGQHY
UNDHU	*NDHUN*	*DHUND*	*HUNDH*	*UNDHU*
YEIVL	FFOOA	JBHQH	UNJLJ	EYXU[illegible]
NDHUN	*DHUND*	*HUNDH*	*UNDHU*	*NDHUN*
FRNYA	DUHGH	YWULW	ENUAY	AXUXQ
DHUND	*HUNDH*	*UNDHU*	*NDHUN*	*DHUND*
HYZED	NYJLL	MVFOY	EGHLN	XMARV

图 6.6:在一篇维吉尼亚密文中,字母组的重复可以透露密钥词长度的蛛丝马迹,这里重复的字母组合是 QHY。

上面给我们提供了一种探寻密钥词长度的方法,从密文中找出尽量多的相同字母组,以及它们之间一定的距离。如果它们源于明文中的相同字母,那么这个距离就是密钥词长度的倍数。

另一个例子是字母组合 PKA,它在密文中两次出现,一次在第八行的第二组,另一次是最后一行的第一组,两次间的字母间距是 144,而且这两个密文组合涉及同一个明文字母组合,即“cht”。我们由此推断,密钥词长度肯定是 52 和 144 的约数。我们先将两个数目分解:

$$52 = 2 \times 2 \times 13$$
$$144 = 2 \times 2 \times 2 \times 2 \times 3 \times 3$$

这两个数字有相同的约数 2 和 $2 \times 2 = 4$。通常人们对 2 不会加以考虑,因为没人会使用这么短的密钥词。那么相同的约

数只剩下 4,密钥词 HUND 的长度的确是 4 位。我们只选取了两个重复出现两次的字母组合,就达到了目的。如果我们对文章进行更为系统的搜索,会发现,VFOYE,LZDA,LFF,FFO 也出现两次,它们同样可以帮助我们获得密钥词的长度。

不过,不能因此而认为,密文中相同字母组合的间距,总是密钥词长度的倍数,例如字母组合 FOU。在图 6.3 的密文中,它出现在第一和第二行,两者间距为 59。这是个质数,没有约数。密钥词长度也不可能是 59,因为它不符合距离重复的 52 和 144。对照相应的明文,我们可以断定,字母组合 FOU 在两处分别代表不同的明文组合,一处是 lbr,另一处是 cha。它们是由密钥词的不同部分加密,一次是 UND,另一次是 DHU,两次碰巧得出了相同的密文字母。在探求密钥词长度时,我们必须小心谨慎并具备敏锐的感觉。

图 6.7 展示了一篇新的密文,我把它分解为 10 字一组。其中,有几个 3 字母和多字母组合出现了两次,EGE 和 ZXE 甚至有 3 次。图 6.8 的表格甚至在字母组合旁注明,重复组合的开头字母处在密文的哪些位置上。右边是差数值,即隔多远组合的开头字母再次出现。这些差数值被分解成约数,以便根据卡西斯基理论确定密钥词的长度。除 IXD,YFG 和第一个值 EGE,其他差值都有共同约数 5。5 极有可能就是我们寻找的密钥词长度。接下来的程序,与前面密钥长度为 4 时完全相同。如果 5 是真正的长度,那么所有第五个字母合在一起,会呈现出单码加密的频率分配规律。事实上的确是 5。寻找明文的任务,我让读者自己去完成——它也摘自《法兰克福评论报》。

BIVLKSGLGY
RRBGYDDTRE
OSLMXUEBXV
PIZIMYRDSD
KVXVJMHPME
XEUEJDEEEE
XSVLEOIWIK
NEDVVSSXEL
ECAWKKBXRU
GEKHVXDBIC
YRMIJLUVLJ
ORWIEQEAIZ

YEGGFNIXVK
GEGRSOSMMD
XIGHVBSIVR
WEGHVCBNGY
NEGFVETXPG
VEBXLXGFMK
JWXMZXEBRR
CANJUONXRA
OSTPGRAUIK
OTMIIXDXWJ
DAUIWEEKFL
WTXBKQEEIX

SSMIZXEGGT
WTXVVQEEQR
MHXHRCHTIL
CTTFVXEXXN
KCAIIRAMIZ
QEUVRMHMQR
XDXVGKSLIE
OWXMCCDBIS
CSMIYONGYE
MHEYVCSXPN
MHLXRLENIS
D

图 6.7:一篇维吉尼亚式密文,其密钥词长度未知。

EBX	67 – 162	$95 = 5 \times 19$
EGE	27 – 40	13
	40 – 270	$230 = 2 \times 5 \times 23$
ENE	130 – 210	$80 = 2 \times 2 \times 2 \times 2 \times 5$
GHV	73 – 103	$30 = 2 \times 3 \times 5$
IXD	285 – 349	$64 = 2 \times 2 \times 2 \times 2 \times 2 \times 2$
IZXE	24 – 149	$125 = 5 \times 5 \times 5$
JMH	125 – 290	$165 = 3 \times 5 \times 11$
MIZ	23 – 148	$125 = 5 \times 5 \times 5$
NGY	108 – 267	$159 = 3 \times 5 \times 3$
QEE	56 – 346	$290 = 2 \times 5 \times 29$
SMI	22 – 262	$240 = 2 \times 2 \times 2 \times 2 \times 3 \times 5$
VRMH	79 – 174	$95 = 5 \times 19$
WTX	51 – 341	$290 = 2 \times 5 \times 29$
XDX	201 – 286	$85 = 5 \times 17$
YEG	11 – 269	$258 = 2 \times 3 \times 43$
ZXE	25 – 50	$25 = 5 \times 5$
	50 – 195	$145 = 5 \times 29$

图 6.8:在图 6.7 的密文中,相同的字母组合重复出现的距离差值。(卡西斯基差数)

在附录 A 中我们可以看到一个简单的加密机，通过它可以使用一个有限长度的密钥词加密，如同使用维吉尼亚法。当然，它们制造的密文与所有多字母替换法加密具有相同的弱点，密钥字母会出现周期性反复。不过，这种机器还提供了利用无限长度密钥词加密的可能性。关于它的优势和弱点，我们会在下一章中接触到。

7

无限密钥词

> 把按照一定规律产生的数字称为"随机数",颇令人诧异……虽然它们的产生方式是完全确定的,但这些数字的特性,却同真正的随机数毫无二致,也就是说,它们看起来像是从一个大彩票箱中抽出来的。
>
> 罗尔夫·J·洛伦茨,《生物统计》

使用维吉尼亚密码为一份文本加密时,密钥词越长,其字母出现频率的典型性越不明显。在上一章中我们已注意到,一个四字母密钥词使得 e 的最高频率由明文中的 17%降至密文中的 9%。密钥词越长,就越难进行统计分析。因此,理想中的密钥词应具有无限长度,或至少不短于明文。这样,密文中就不会留下某种节律的痕迹,而正是这种节律,可以帮助破译维吉尼亚式密文。

作为绦虫式密钥的《苏菲的世界》

假如我们把密钥词作得同明文一样长,那么置换密钥就如同置换明文一样困难。我们可以自寻出路,选取一篇文章充当密钥词,这篇文章应出自一本普遍可以理解的书籍,而且密码发送双方必须都熟悉它。譬如我们可以采用哲学历史方面的畅销书,约斯泰因·戈德尔的《苏菲的世界》。这样这个密钥词就近乎一条无限长的字母虫:

SOFIEAMUNDSENWARAUFDEMHEIMWEGVON DERSCHULEDASERSTESTUECKWARSIEMIT JORUNDZUSAMMENGEGANGEN...

这样毫无间断地写下去,经过606页,直至结束:

... *BOOTSCHWIMMERWIRSCHWIMMENBEIDEPAPA*

传递密码时,我们并不需要把整本书都寄给接收者。我们只需告知:"《苏菲的世界》,1993年德语版。"接下来我们就可以向他发送信息了,大意是:

wirsindpleiteraeumedensafekommeueberzuerichnachsantiago

〔但愿他会念成"zuerich nach santiago",而不是"zu erich nach santiago"。〕密钥的第一个字母是S,于是我们查找维吉尼亚密表(图6.1)的S行,w下面是O。下一个密钥字母是O,我们来看表中的o行:i下面为W……这样逐个密钥字母,逐个明文字母地进行下去。最后一行密文就出现在我们面前:

OWWAMNPJYHAXRNAVUGJGIZSENOGSSHSHHFVJBBYCMFHFETZ
LEFMCEIY

在密文中根本找不到密钥词留下的节律痕迹，除非密文的页数多于 606 页，而且加密者可以从密钥书的结尾返回开头。

这则消息的加密真的那么安全吗？在较长的密文中可以看出，不仅明文，而且连密钥文也具有德语的特征。即使文章摘自外文书，如原版的詹姆斯·邦德小说，这也帮不了多少忙。在这种情况下，密文同样会呈现出一种频率模式，不过是英语的。让我们回到德语密钥，由于密钥文中的 e 和明文中一样，是最常出现的字母，因而 e 经常由 E 行加密，结果密码字母 I 往往具有高频性，正如图 6.1 所示。明文中频繁出现的字母组合，如 en，经常同密钥文中的一个常见字母对相遇，反映在密文中就成了字母对的重复。结论：明文和密钥文的字母频率模式会在一篇足够长的密文字母频率模式中反映出来，并使窃码变得容易。不过无论如何，这比破译简单的维吉尼亚密文费力。

当然，在下面的密信中，我们当然不可以再从绦虫式密钥的那个开头，即从 SOFIE…开始。否则所有密信的第一个字母都用 S 来加密，这会形成以德语字母表为基础的单码密码。这对后面的密码字母也一样，所有的第二个字母会以 O 加密，第三个则是 F，以此类推。如果获得足够多的信息，我们就可以通过频率分析进行脱密。例如，破译者从上百篇截获的密件中，抽取每篇的第一个字母，确定它们的频率性，从中可以发现，哪些密文是以明文字母 e 开头的。然后他对所有信息的第二个字母进行同样操作，接着第三个，一直进行下

去。通过这种方式，他应该可以找出所有密件中的明文字母e，然后再寻求第二位最常见的字母n。花些力气，再加上点感觉，他就可以成功地破译所有密文。

所以，发信人在下一封密信中，应选取绦虫式密钥中另外的点作为开端。每隔一段时间，他可以使用密钥书的新一页，定期更换。当然，诸如“一天一页”的约定，必须在交换密钥时通知接收者。如果在每则密信的开头标上此时使用的页码，并且未加密，这是极其危险的。

不一定总是凯撒密表

无论是使用短密钥词，还是用一本书那样长的绦虫式密钥，到目前为止我们还停留于维吉尼亚式类推字母密表。这种方法在127页的解密中向我们提供了帮助，但并非实质性的。密钥词的长度是关键。如果知道了长度，我们就可以推测出哪些字母是以同一单码方式加密的，至于这些相对独立的加密方式是否为“凯撒密表”，并不重要。无论如何，它们都是单码式，只要手头有足够篇幅的文本，就可以破译。假如我们使用的密表不是逐行推移式，而是随意编排的，如图7.1所示，那就能给入侵者制造些麻烦。倘若我们决定这样做，那么我们不仅要交给接收者密钥词，更要给予整张密表，推移字母表形成的维吉尼亚密表的最大优点在于，我们无需任何其他辅助手段就可以将其复原。即使在牢狱中，也可以把心中默记的维吉尼亚密表，用折断的勺子刻到墙上，而对图7.1中的密表就行不通。

在维吉尼亚式加密中，使用有限的密钥长度编出的密文，会泄露密文中密钥的节律。即使使用任意长度的密钥在密文

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	E	N	A	M	O	F	L	P	D	K	Q	C	J	Z	R	Y	G	X	I	W	S	V	B	U	H	T
B	L	Y	F	Q	X	R	E	G	K	U	N	O	A	P	S	D	B	C	[illegible]	V	I	H	W	Z	M	J
C	S	C	R	T	A	H	U	Q	G	V	I	P	W	D	F	X	O	J	Y	N	B	Z	M	L	E	K
D	Q	G	P	R	A	O	S	F	N	Z	T	H	Y	B	X	U	W	M	E	V	L	I	C	K	D	J
E	R	G	Q	C	Z	P	F	O	T	B	N	H	U	L	E	S	M	K	V	Y	A	J	X	D	W	I
F	H	N	A	G	O	M	B	P	Z	I	L	Y	Q	X	F	W	C	V	R	U	K	T	E	S	J	D
G	S	I	A	R	T	H	J	Q	U	C	O	P	V	K	G	B	W	N	F	M	X	E	L	Y	D	Z
H	Z	L	Y	D	E	X	K	M	W	C	J	V	N	F	U	I	O	T	[illegible]	S	H	R	G	Q	P	A
I	L	I	P	K	M	O	Q	H	J	N	Z	R	A	Y	G	B	X	S	F	W	C	E	V	T	D	U
J	O	X	L	E	W	Y	N	K	V	Z	P	A	U	M	B	T	Q	J	[illegible]	F	I	R	C	H	D	G
K	Z	N	H	Y	A	M	X	O	J	W	B	L	V	P	I	U	C	K	T	Q	D	S	E	F	R	G
L	L	X	F	N	W	Y	K	A	V	Z	M	O	U	B	R	J	G	S	P	C	R	I	D	Q	H	E
M	O	G	N	A	P	B	M	Q	H	C	R	L	D	Z	S	I	K	Y	T	E	X	F	W	U	J	V
N	N	G	X	A	M	Y	O	F	W	Z	Q	L	V	S	H	U	P	R	T	K	E	J	B	I	C	D
O	Y	M	X	F	L	W	N	A	V	H	K	U	O	C	T	J	G	S	Z	P	I	R	B	E	Q	D
P	F	L	E	M	K	G	Z	N	Y	J	X	A	W	O	V	I	U	D	T	P	S	H	R	C	Q	B
Q	T	F	U	S	I	V	R	C	W	Q	H	Y	P	E	X	O	J	Z	N	G	M	B	L	D	K	A
R	W	B	E	H	I	R	K	N	P	Z	M	J	S	T	U	A	Q	O	V	X	L	C	Y	F	G	D
S	I	X	E	W	Y	H	V	Z	J	U	A	T	[illegible]	S	K	R	D	Q	F	P	L	O	B	N	C	M
T	A	X	L	W	Y	I	V	Z	K	E	U	M	H	T	J	S	D	R	N	W	G	P	B	F	O	C
U	Z	C	E	Y	H	D	X	G	M	W	I	L	V	N	U	B	T	K	S	O	R	F	J	Q	A	P
V	Z	J	Y	G	X	F	W	K	V	I	U	A	T	L	S	H	R	E	Q	M	P	B	O	D	N	C
W	N	F	M	O	E	L	P	H	Z	K	Y	Q	X	D	W	J	V	B	U	G	T	I	S	C	B	A
X	A	N	B	M	O	C	L	P	D	Z	K	Y	Q	X	E	W	J	V	R	U	F	T	I	S	G	H
Y	I	R	B	H	Q	S	J	A	P	T	Z	G	Y	O	K	X	U	N	W	D	M	V	F	L	C	E
Z	K	T	J	B	S	U	A	L	R	V	I	D	Q	W	C	M	P	X	H	F	O	Y	E	N	G	Z

图 7.1:一张由许多随意打乱的字母表组成的维吉尼亚密表。上面依然是明文字母表,左边表外是密钥字母。如果密钥词是 HUND,我们就从第八行开始,然后依次采用第 21、14、4、8、21、14、4、8……行。这时,脱密更为困难,因为没有凯撒推移式密表可供参考。不过这同时也给密钥的秘密交换增加了难度。

中也会反映出明文和密钥的语言规范性。如果我们使用的密钥文不会泄露任何节律或突出个别字母，如：

AJKZFBIXRCBWWHF...

那么就可以避免这个薄弱环节。当然，如此一来，我们就不能从书籍中，比如《苏菲的世界》中截取绦虫式密钥，而是自始至终由随意拼凑的字母组成的书中去寻找。它们永远不会成为畅销书。

在实际操作中，人们还可以用数字来代替字母。我们已看到，凯撒推移式密表很容易用数字来表示，只要将每一个字母，不管它在明文还是密文中，与它在字母表中的位置对应起来。也就是说，直接用01、02、03、04……来代替a、b、c、d……。在密码学中，还有一种方法很常用，它已有2000多年的历史了。

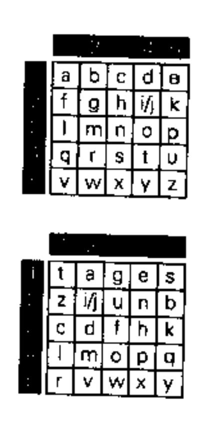
波利比乌斯密表

希腊诗人及历史学家波利比乌斯生于约公元前200年，逝于约公元前120年。他编写了首部世界通史，共有40卷，其中5卷留存了下来。另外，他还从事密码学方面的研究，直至今日，还有一种加密法被冠以他的名字。

如果人们不分明文字母i和j，就可以借助棋盘的形式，得到一种数字式加密法(图7.2上表)：g变为22，p为35，等等。

如果不是按照字母表的顺序，而是以任意一种其他的顺序来排列密钥表中的字母，那么窃码者制造的困难就更大了。当然，这事先要告知接收者。一般来说，我们可以先把密钥词

的字母写入表中的前几格里，然后用剩下的字母补足其他的格(图 7.2 下表)。但紧接着我们将利用上面那张较简单的密表加密。“tabak”会变为 44 11 12 11 25。



a	b	c	d	e
f	g	h	i/j	k
l	m	n	o	p
q	r	s	t	u
v	w	x	y	z

t	a	g	e	s
z	i/j	u	n	b
c	d	f	h	k
l	m	o	p	q
r	v	w	x	y

图7.2：波利比奥斯密表。上表：字母表式填充。下表：利用提示词“Tageszeitung”填充。每个字母对应一个数对。依照上面的密表，e 变为 15，m 为 32。波利比乌斯密表提供的是一种单码加密法——每个字母只能分配到一个数对——但它提供了一种简便的方法，使我们可以通过算术式编密，将一篇字母文章变为数字文章。

这种加密方法曾为沙皇时代俄国的囚犯所利用，他们相互间通过敲击牢房墙壁交流信息。不过，他们使用的正方形为 6 行 6 列，而不是 5 行 5 列，以便表示旧西里尔字母表中的 35 个字母。这种描述方法由沙皇统治的反对派“虚无主义者”得名，被称为“虚无主义式”。字母表中的每个字母都准确地对应一个数对，反过来说，收到的每个数对肯定代表一个明文字母。

这种加密法不是很可靠。窃密者很快就会注意到，每份密信都由总量为偶数的符号组成，而且只有数字 1 至 5(在虚

1

2

14

无主义式中为1至6)出现。他们可以据此推测，每两个数字对应一个字母。由于被使用的5个数字只能组成25个不同的数对，这等于说，每个明文字母同一个数对对应。于是马上可以断定，这是否是一份单码密码。在一篇足够篇幅的文章中，25个可能出现的数对中，代表e的数对出现应该最频繁。破译者可以像对待所有其他单码加密法一样，顺着这个思路做下去。他很快就会得到一份复原的波利比乌斯密表，即使结果是图7.2下面的那种随意编排的字母表，也同样可以获得。今天，人们大多采用波利比乌斯表的方法，将字母序列转换成数字序列形式。

数字绦虫式加密

现在我们来为《苏菲的世界》的一篇文章加密，但使用数字。

我们采用的明文是：

wirsindzahlungsunfaehig...

借助波利比乌斯正方形(图7.2上表)，我们得到一篇"数字式"明文，即：

52 24 42 43 24 33 14 55 11 23 31 45 33 22 43 45 33 21 11 15 23...

这样我们首先得到了一份单码密码。然后我们再从《苏菲的世界》中选取密钥词：

S O F I E A M U N D S E N W A R A U F D E M...

并利用波利比乌斯密表把它转换成一个“数字式密钥词”：

43 34 21 24 15 11 32 45 33 14 43 15 33 52 11 42 11 45 21 14 15 32…

接下来是个简单的算术题目。我们把明文和密钥词分上下写到一起，两者都以数字的形式。然后我们把它们加在一起，不考虑十进位制，如图 7.3 上部那样。这样我们就得到一篇数字式密文。如果不清楚密钥词，破译它并不是件易事。

52 24 42 43 24 33 14 55 11 23 31 45 33 22 43 45 33 21 11 15 23 …
43 34 21 24 15 11 32 45 33 14 43 15 33 52 11 42 11 45 21 14 15 …

95 58 63 67 39 44 46 90 44 37 74 50 66 74 54 87 44 66 32 29 38 …

95 58 63 67 39 44 46 90 44 37 74 50 66 74 54 87 44 66 32 29 38 …
43 34 21 24 15 11 32 45 33 14 43 15 33 52 11 42 11 45 21 14 15 …

52 24 42 43 24 33 14 55 11 23 31 45 33 22 43 45 33 21 11 15 23 …

图 7.3 上：根据图 7.2 上部分的波利比乌斯密表转换成数字形式的明文“wir sind zahlungsunfaehig”，借助同样被变为数值绦虫形式的密钥词(SOFIEAMUNDSEN…)，再编成数字式密文。下：相应的脱密。

那么接收者该如何处理这封密信呢？他把数字式密钥词写到密文下面，如同图 7.3 下一样作减法运算，但不用十进位制。这样他就得到了数字式明文，再通过波利比乌斯密表，就可以把它转换成可读的形式。数字式加密法与字母加密法和维吉尼亚密表加密法大同小异。同字母法一样，明文和密钥文中的某些先选的词会在密文中留下痕迹。为避免这种情况的发生，人们须用一种随机抽取的无意义字母组合或随机的数字序列作为密钥词来替代正常的语言。

偶然性没有记忆力

第一次世界大战失败后，德国人面临着重建国家的任务。1919年2月6日，国民议会召开大会，成立魏玛共和国。当时设立新的外交机构势在必行，为此急需一种新的加密方法，以便驻外大使馆可以利用它同国内政府互通加密信息。新的国家应采取什么方法加密？维尔纳·孔策和鲁道夫·绍夫勒探究了这个问题。前者是位数学爱好者，后者是位致力于语言研究的密码学家，后来还获得了数学博士学位。与这两位志同道合的还有化学家埃里希·朗洛茨。根据当时官方的加密法，通常是在明文转化成的数字序列后，缀上一个没有十进位转换的数字式密钥，大概如我们在图7.3上的做法。这三个人着手调查这种加密法的安全度，很快他们就得出结论，对于一篇足够长的文章，即使密钥为40或50位的数字序列，也不足以对窃码者构成障碍。在他们看来，只有不加重复的随机数字序列能保证绝对安全。因而外交机构配有50页的密码本，其每页带有由随机数字组成的85个五位数组。没有完全相同的两页，而且每页只准使用一次。消息加密后，所用的那一页必须销毁，对于下一则密信则使用下一页。后来，这种方法也被引入别的国家。在英语国家中，它被冠以“一次性密本”的名称，暗示其每页只能使用一次。

如果人们严格遵守它的规则，这种方法是绝对安全的。对于这么大篇幅的文章进行分析，不可能得到关于密钥的信息。它的缺点在于，涉及范围太广。整本密码本总有很多页，发送者必须通过某种秘密途径把它传递给接收

者。

苏联的秘密情报机构在第二次世界大战后还在使用这种加密法。1953年6月20日,美国的一对夫妇埃塞尔和朱利叶斯·罗森堡被处决于纽约新新国家监狱。两年前,他们因泄露核机密的罪名被判处死刑。他们充当苏联间谍,一个失误导致他们暴露了自己的身份。苏联人多次重复使用一篇密钥文,连负责的官员也不得不为此错误付出生命的代价。[1]

前苏联的秘密机构也使用随机抽取组合而成的密钥文,具体地说:是由所谓的"随机数"组成的数字序列。表Ⅱ中就是这样一个密钥。1957年6月,当苏联间谍鲁道夫·艾贝尔在纽约旅馆被捕时,美国联邦调查局的一个密探发现了一个密本,其如邮票大小的纸片上,密密麻麻地写满了长长的数串,这是数字式绦虫密钥。在五六十年代,其他苏联间谍在被捕前也不能及时销毁密钥。美国人很快就发现,这根本不是真正的随机数字,因为它们包括太多这样的数串,其中由一组1、2、3、4、5组成的一个符号同一组6、7、8、9、0组成的一个符号交替出现,例如数串291738。很明显,这是由打字机前的女秘书用左手和右手交替在键盘上敲击出来的,她左手负责一组数字,而右手负责另一组。一个数字极少重复或者先后3次出现。显然,不管谁制造密表,他显然或下意识地认为,重复2次甚至3次就违背了随机的原则。而正如我们所知,真正的偶然性并不回避重复。

看起来正是俄国"随机密钥文"的这种特性,在1991年8

---

① 《新科学家》,1995年7月22日,第42页。

月制造了世界历史。当时在针对旨在推翻米哈伊尔·戈尔巴乔夫政权的政变中,两位叛乱者,克格勃头子佛拉吉米尔·克留奇科夫和国防部长德米特里·亚佐夫,互通密信,美国人恰恰根据密钥中的规律性破译了这些密信。布什总统将结果转交给鲍里斯·叶利钦。

写下一串数字,不突出其中任何一个,这看上去很简单,例如 08297321870134,但我们会特别偏爱某个数字,而自己毫无察觉。人们在选用一个新数值时,总会不由自主地回想前面的数字,并尽量避免重复。而随机性则相反,它并不记得前面发生的事。如果你想得到一篇安全可靠的密钥文,就不能相信"人为的"随机数。

许多游戏规则都建立在这样的基础上,即认为随机性是有记忆力的。假如在轮盘赌博时,有人认为 15 不过是被"轮到"了,因为小球已避开它 100 次,那他就大错特错了。在一个理想的轮盘赌台上,中心的小球会以同样的频率碰到所有可能的数字,但它并不会因此而得到调整,在 100 次之后会"纠正"先前的无规律状况。

彩票数字的产生也是随机的。这周会产生什么数字,并不取决于上周的结果,然而还是有很多参与者确信,一个长时间未被抽到的数字,占有更大的机会。图 7.4 是从一份德国日报中摘录的,其中的图表为读者参与下一局出谋划策。谁郑重其事地认为,35 应被看好,成为下一批中奖数字,因为它已经有 37 个周未被抽到了,如果他真这样做的话,那就错了。

人们不能凭感觉制造随机数。只有真正的随机方式,比如从帽子中抽纸条,掷骰子或客观地计算操作,才合乎要求。

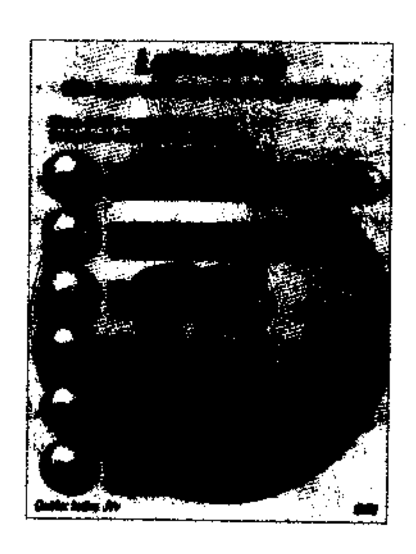


图 7.4：一张帮助读者填写彩票数字的图表，它暗示读者，一个长时间未被抽到的数字，如 35，与一个也许上周正巧属于中彩的数字相比具有较大的概率，会在下一次被抽中。

偶然——人为制造

有许多方法可以制造随机数字，比如，我可以把数字 0 至 9 写到小纸条上，将它们都扔到一顶帽子里，然后闭着眼睛，每次从中抓一张，抄下纸条上的数字，再把它扔回去，摇一摇，再抽出一张。这样耐心地进行下去，就可以得到一串随机数据，它们可以充当绦虫式密钥。

然后我把绦虫式密钥的复印件寄给一位将来可能接收我密信的人。假如我需要向他传递一份密信，首先要把明文根据波利比乌斯密表改编成数字串，再补加上一个无十进制的数字绦虫式密钥。这样我就得到一篇数字式密文。那位接收者现在拥有我从帽子中抽取的绦虫式密钥，于是就可以从密文中减

去密钥文(还是不考虑十进位制),得到数字式明文,再借助同样的波利比乌斯密表,就可以把它复原到字母式明文。

我用秘密方式传递给接收者的密钥文,同需交换的密信一样长。[1] 这似乎也占不了多大便宜,因为密钥文落入窃码者手中的概率,同明文落入他人之手的概率一样大。

正如我们在第一章中所见,R·佐尔格身边的间谍网没有使用事先做好的随机数密钥表,而是利用一本统计年鉴中的数字,其优点在于,在房间被搜查时,不致因用途不明而引人注目。而一张人们无法解释其用途的符号表会引起人们怀疑。此外人们可以避免交换冗长的数串,而只需一个简短的提示,如"书 XYZ,12 页"。只要提示接收者一个短数,他就可以利用它制造出一串长长的密钥词。

我们举一个简单的例子,用 7 除 1,商的位数就可以趋向无限:
1/7 = 0.142857142857142857142857142857……

这是一个循环小数,循环部分由数字 142857 组成。我们可以把这 6 个数字看作随机数,充当一个简短的绦虫式密钥。举例来说,我们给原文第 163 页明文的第一个词"wir"加密。借助波利比乌斯密表(图 7.2 上表)先把它变为数字式明文 52 24 42。接着我们把数字式密钥词写到它下面,并加起来:

52 24 42
14 28 57...
66 42 99

对于这种密文,接收者可以通过减去密钥数字,将其还原

---

① 如果使用类似图 7.2 那样的波利比乌斯表,我还必须考虑到,接收者是否已得到了密钥词或提示词。

为数字式明文。这里密钥词无足轻重,因为它太短了。但还有其他数字,它们在被除时,得出的结果在出现反复之前,就已得到了一长串数字。我们来看数字 499,分数 1/499 可以提供 498 个非循环数字,也就是说从第 499 个数字才开始循环。我们可以用它为较长的密信加密,接收者只要得到数字 499 作为密钥,他就可以制造出一个数字式密钥。

有些小数更为合适,它们产生的数字串中根本不存在循环。最著名的数字是 π,即圆的直径同周长之比:

$$\pi = 3.141592653\cdots\cdots$$

数学家知道,在这组数字中没有循环(图7.5)。虽然有

Volume 7 Number 3 1985 $4.95

The Mathematical Intelligencer

1415926535 8979323846 2643383279 5028841971 6939937510
5820974944 5923078164 0628620899 8628034825 3421170679
8214808651 3282306647 0938446095 5058223172 5359408128
4811174502 8410270193 8521105559 6446229489 5493038196
4428810975 6659334461 2847564823 3786783165 2712019091
4564856692 3460348610 4543266482 1339360726 0249141273
7245870066 0631558817 4881520920 9628292540 9171536436
7892590360 0113305306 4882046652 1384146951 9415116094
3305727036 5759591953 0921861173 8193261179 3105118548
0744623799 6274956735 1885752724 8912279381 8301194912
9833673362 4406566430 8602139494 6395224737 1907021798
6094370277 0539217176 2931767523 8467481846 7669405132
0005681271 4526356082 7785771342 7577896091 7363717872
1468440901 2249534301 4654958537 1050792279 6892589235
4201995611 2129021960 8640344181 5981362977 4771309960
5187072113 4999999837 2978049951 0597317328 1609631859
5024459455 3469083026 4252230825 3344685035 2619311881
7101000313 7838752886 5875332083 8142061717 7669147303
5982534904 2875546873 1159562863 8823537875 9375195778
1857780532 1712268066 1300192787 6611195909 2164201989

图 7.5:π 值小数点后的前 1000 位。摘自柏林/海德堡斯普林格出版社发行的一本杂志扉页。

个别数字甚至数组多次出现，但每次其中总间隔着别的数字。1995 年，东京大学的数学家把 π 值精确算到 32.2 亿位，他们还因此而打破了当时 6700 万位的世界纪录。他们的大型计算机为得到这个数值需要工作 36 小时 51 分钟。利用 π 值数组，可以加密任意长的文本。就目前所知，其中没有任何数字被突出，至少人们没有发现任何规律。使用 π 值，您可以放心大胆地加密。不过您必须向接收者提供线索，使他知道该取小数点后多少位数字，这样他才可以解读密信。您还可以使用 2π 或 7π，数学家知道很多类似的无限数能用于加密。

随机数组对其他用途也很重要。因此，数学家发明了一些方法来制造随机数，即制造无循环，无突出数字的数组。其原则在于，从一个原有的数字中，英语称为“seed”，即“种子”，通过某种算术方法，造出一个新的数字。而它又可以充当下一个数字的种子，同样再下一个数字也可以用于再下一步操作，这样可以无限继续下去。而这些数字是否能以这种方式平均分配，且不至于陷于一种循环结果，取决于计算方法。人们将这类计算程序称为“随机数生成程序”；今天，几乎所有的计算机中都存有这种程序。许多电脑游戏也利用了随机数，但这些并不是真正随机的。由于计算机中的数字长度有限，因而它所提供的数字虽然是巨大的，而且相互不同，但依然是有限的。总有一天，数据生成程序会制造一个已被它用过一次的“种子”。从此，“种子”开始周期性重复。较差的随机数生成程序的循环周期很短，而好的则很长，在几十亿轮之后，结果才开始重复。图 7.6 中的数字序列，是我在可编顺序控制中用随机数生

成程序制造出来的。[①] 确切地说：我制造了随机数，从中得到了一条绦虫式数字。我把 0 选为种子，第一个数对是 39，然后根据脚注中的规则，随机数生成程序可以不停地提供新数对。

```
3907636928805230911090050807776
9230363455870399626300697421175
4328956012282445349646164974779
4823405140859213506278581977794
9801185874959964318171417422640
2654817531802701349497671754883
4399640684324697969078179438831
1033476279485288097166008699951
2266555907611423828173943624772
7246555710321270764616076261333
1650349584469693780013751845992
7378160431834276096972427796333
4807030174830187047605360867786
1502949739201141148398172787705
5124319690185876345502376717997
1121910915437122234399805243997
1287014997138929722913787605449
5608949529280746838239348223998
1727459333781844876429285286996
5166405587217286417504864370778
5609692957950399070356921545336
9036478883672085345647190448994
```

图 7.6：由一个随机数生成程序制造的随机数。

① 我把种子乘以 5，再加 123456789，得到的结果，用模 2^{20} 去除，取余数，于是得到一个数值 S。S 的倒数第三个和第二个数字组成我的第一个数对。数字 S 则充当制造下一个数对的种子。

现在,我们可以重新加密原文163页上的数字式明文。我们从图7.7上的字母式明文入手,把随机数字或密钥写到下面,再叠加,且不考虑十进位制,这样就产生了数字式密文。如图7.7下所示,接收者把密钥数字写到数字式密文下面,再做减法运算,由此他得到了数字式明文,然后根据波利比乌斯表把它还原为字母式明文。

522442432433145511233145332243453321111523...
390763692880523091109005080776923036345587...
812105024213668502332140312919376357456000...

812105024213668502332140312919376357456000...
390763692880523091109005080776923036345587...
522442432433145511233145332243453321111523...

图7.7 上:用图7.6中随机数的绦虫式密钥的开头部分加密;下:相应的脱密。

当然,在这种情况下,接收者必须具备相同的随机数生成程序。交换密钥时,我须先告诉他种子为0,如果需要的话,还要给出波利比乌斯密表的提示词。这样他就可以解读我的密信了。我们在交换密钥时,只要传递少量信息,就可以交流任意长的密文。当然,我用种子数0选一个数,在实际情况中没有人会用它。我也曾以4562183170作为第一个种子进行加密,这是一个十位数字,可以产生一百亿种不同可能性。如果谁企图采用木锤加密法,检验所有可能的种数,以便能碰到一篇可读的明文,即使每种情况只需一秒钟,他也必须夜以继日地工作三千年。

电话号码簿中的絛虫式密钥

英国记者罗伯特·马修斯介绍了一种简单的方法，可以不费吹灰之力就从随机数字中得到一个絛虫式密钥。① 他选了一本伦敦地区电话号码簿，上面约有120万个7位数的号码。它们是按机主姓名的字母顺序排列的。前3个数字同伦敦电话网中的汇接点有关，取决于其所属区域。如果所有取亚洲名"帕特尔"的人都住在同一个区，那么电话号码簿中会出现一连串开头一样的号码，因此电话号码簿中号码的前几位数字并不是随机性的，但后几位数字则不同。马修斯用自己的个人电脑从各个角度对它们进行了检测，证明最后两位数字完全是随机数字，用它们很容易制造出絛虫式数字。

人们取一本大城市的电话号码簿，从某个电话用户开始，记下号码的最后两位数字，然后再看紧邻的下一个，照此进行下去。通过这种方式，我们可以得到一个絛虫式密钥，如果接收者已知道作为密钥的城市名和用户名，那他完全可以以同样的方式制造出这组数字。

马修斯还解释了如何自己动手作一个简单的加密机，这种加密机可以使用一些如维吉尼亚密表的有限密钥词，或诸如源自电话号码簿的任意长度絛虫式密钥。附录A就介绍了这种机器。

① "一种用于周期或随机密钥加密的转筒装置"，《密码学》，1989年，第266页。

1
4 4
5

8

打乱的文本

在《花园篱笆》中有一行著名的中学生密码，明文字母按顺序上下交替写成两行。“man hat uns entdeckt bring dich in sicherheit”可以写成

m n a u s n d c t r n d c i s c e h i

a h t n e t e k b i g i h n i h r e t

于是就成了 MNAUSNDCTRN…

《不列颠百科全书》

1609 到 1610 年的冬天，意大利天文学家伽利莱奥·伽利略把他的望远镜对准浩翰星空，他发现，那条朦朦胧胧的银河事实上由无数闪烁着微光的星星组成。他还观测到，木星由 4 颗卫星环绕；在月亮上，山峰的阴影投射到广阔的平原上；太阳表面有黑子。在他看来，土星这颗行星似乎由 3 颗星组成。这都是轰动性的新闻。伽利略抢先采取行动，确保自己在这项发现上的优先权，也正如今天的科学家所做的那样。

换序构词法

当时的学者们通用的方法是，既不“和盘托出”又能获得首次发现的荣誉。他们把自己的事迹浓缩到一个简短的句子中，大多为拉丁语，然后通过打乱句子中所有字母的顺序给这个句子加密。例如他们有时干脆按字母表来排序。通过这种方式为句子加密，是很容易的。譬如，“siriushateinenbewohntenplaneten”，将字母按字母表顺序排列，就形成密文，[illegible]。要想从中复原明文，在实际上是行不通的。但如果别人也发现了这颗行星，你可以通过字母的排列组合来证明，你在此之前已发现了它。这样就没有人能对你首次发现的荣誉质疑。

这种加密方式被称为“换序构词法”。字母排列不一定非要按照字母表进行，明文字母顺序可以随意调换。关于发现土星，伽利略的拉丁语明文句子是这样的：

altissimum planetan tergeminum observavi

译成德语，就是“我观测到了具有 3 种形态的最高行星，”这里“最高行星”指土星。在当时的世界天体图上，这是绕太阳公转的最远的一颗行星。然后他通过调换字母位置，把这个拉丁语句编为密码形式，他的发现就是以字母序变文的形式发表的[1]：

SMAISMRMILMEPOETALEUMIBUNENUGTTAUIRAS

没有人能从中读出某种意思。然而一旦另外一名天文学家突

① 在此，伽利略没有区分 U 和 V。

然跳出来声称，他已观测到了3种形态的土星，这时伽利略就可以骄傲地指出，他早已将这个发现写进了他的回文构词法。于是另一个人就被击败了。伽利略通过这种方式，把自己的许多发现编成密码。虽然在上面关于土星的句子中，他的加密非常成功，但明文内容却并不正确。半个世纪以后，荷兰天文学家克里斯琴·惠更斯才认识到事实，他用一句拉丁文写下这个发现，译成德语为“它的周围环绕着一个扁平的环，两者间没有接触，环向黄道[①]倾斜”。他简单地依照字母表顺序排列明文字母，3年后才公开谜底。

打乱的文本对打乱的字母表

字母序变文加密的规则，确切地说是反规则，同第四章的单码加密有着本质的区别。在单码加密中，字母表被掩盖，产生一个密码字母表，同正常排列的字母表相对而设，如图4.6所示，e变为F，k变为G，等等。这里有可能借助密文字母的频率性找出明文中的e。而在字母序变文中改变的不是字母表，而是明文本身。让我们来看第五章中的那篇明文：

inderregelfaengtmanmitfuenfziganderweltsattzuwerdenabermit
sechzigistdieweltmuedeanunsgeworden

我们像伽利略那样把它变为字母序变文：

AAAAAABCDDDDDDEEEEEEEEEEEEEEEEEFFFGGGGGHIIIIIILLLM
MMMNNNNNNNNNNORRRRRRSSSSTTTTTTTUUUUWWWWZZZ

无论是在明文中，还是在通过换序得到的变文词中，e还是

---

① 黄道就是地球按照自己的轨道绕太阳公转的平面。

E。变文词不是用来传递密信的，它的作用在于保证优先权。

我们可以确定：在此方式中，明文中的字母仅仅是被移到另一个位置上，这叫做移位法。在第四至七章和第九章及以后介绍的方法中，字母保留自己的位置，但由另一个字母或符号取而代之。把密码学变成了一门科学的是数学家，他们提出置换一说，正如我们在第一章中已有所了解的那样。简单地说：在移位时，明文被随意编排；而在替换时，字母表被随意编排。

由于字母在移位时，并没有被别的字母取而代之，因而密文中最常见的字母依然是E，第二位还是N，但这类知识对窃码者却没有什么帮助。不过，至少经过移位加密的文本对他还有一点用。如果他能确定，这里字母的使用频率同德语中字母的频率比例相吻合，他就可以断定，这是一篇德语明文的移位。如果不是E，而是A成为出现频率最高的字母，那么明文可能是葡萄牙语。如果E出现最频繁，而且N处于第二位，那么他极有理由推测，明文应同德语有关，而不是英语，因为在英语中处于第二位的字母应该是T。

如果我们想通过移位来加密情报，那么我们选择的规则，应同样有利于脱密。第一章中的桑道夫伯爵的编码框，就是一个例子。

奥地利上校的编码框[①]

1885年儒勒·凡尔纳写了小说《桑道夫伯爵》，在此之前4年，奥地利上校爱德华·弗莱斯纳·冯·沃斯特罗维茨发表论文《新佩特伦密码》，这里“佩特伦”(Patronen)一词不是指弹壳或

① “编码框”在密码学上称为“旋转漏格板”。——译者

蘸水钢笔的墨水囊，而是指方格纸上的图纹，这是纺织业中使用的一个名词。

弗莱斯纳在文中描述的编码框，是一个由一系列漏格组成的正方形，如图 1.3 所示。它的行数和列数均为偶数，这样小格的总数就能被 4 除尽。小格的 1/4 要被剪掉，这种编码框既可用于加密，也可用于脱密。脱密时，必须将原文写在与编码框大小相同的正方形内。

在加密时，将编码框置于一张空白纸上，然后逐个字母地将明文写入空格中。填完这些空格后，把编码框按顺时针方向旋转 90 度，再在空格中填写。依此类推，直至编码框转过 4 个方向为止。编码框的制作原则在于，将方框的所有小格写完之后，不会有小格被重复填写。如果文本较长，我们可以再设置一个同样大小的方框。方框的剩余小格内，可以随意填入字母。最终的密文，如桑道夫密文，由正方框的所有字行组成。

在脱密时，我们可以把编码框置于密文的第一个正方框之上，读出可见字母，将它们记录下来。然后把编码框旋转 90 度，依次类推。然而不是每个编码框都适于这种操作。在 4 个角度上，同一个小格不许显露两次，但也不可以根本不显露。

弗莱斯纳编码框无法提供十分可靠的加密方法。密文的字母总数暗示了编码框中的小格数量。譬如说，如果密文由 108 个字符组成，这就可以推测，它来自于大小为横竖 6 格的方框。如果我们掌握了方框的大小，且有足够篇幅的文本供使用，我们就可以查明，在编码框中有多少小格被剪掉了。虽然字母都是照此排序的，但编码框所能提供的也只是一种置换——e 还是 E，n 还是 N。接下来对我们有用的是字母组对。德语中，en 是出现频率最高的字母对，c 和 h 也经常成对出现，同样的还有 c 和 k。

事实上,图 1.4 的第一个密码方框中,C 处于第一行的第一位时,H 是第一行的倒数第二位。而在图中的第二个方框里,C 和 H 则分别处于第五行的第一和第四位。这引导我们推测,在某个角度上,编码框第一行的第一和第五格是开放的,或者第五行的第一和第四格是开放的,而中间的格则是封闭的(否则,H 不会直接跟在 C 之后)。事实上,桑道夫编码框按顺时针 3 次旋转 90 度后,在第一和第五行被推测的位置上的确有空格。通过这种方式,再借助密文中的数对,就能猜出用于加密的编码框的某些特性了。有了足够长的密文,弄清编码框的所有空格,只是一个时间问题。

如果把编码框反过来,使它同目前的位置呈反射对称状,那么脱密就更加困难。这样就能将目前得到的密文,以编码框的方式再次加密,如图 8.1 所示。对一篇已加密的文本进行二次加密,被称为"重叠加密"。不过,无论人们多么频繁地旋转编码框,e 依然还是 E。

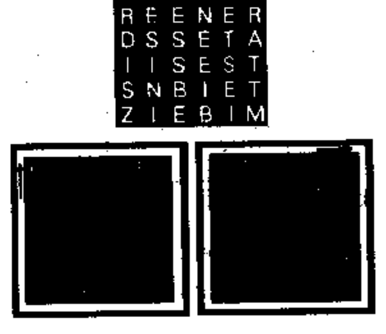


图 8.1:由弗莱斯纳编码框制成的密文可以被再次加密。我们把已加密的文章,再次写入一个方框,如图 1.2 所示,把同一个编码框再利用一次,不过这次是用它的背面。现在所有的空格,都同第一次加密时用的编码框正面空格反射对称。我们再次按 4 个角度依次把它置于字母方框中。第一个方框提供了一份新的密文:CEHEEISSE,如果按顺时针方向旋转 90 度,就得到 ALEEDAEBT。

我怎样为自己制作一个弗莱斯纳编码框呢？我应该剪掉哪些小格，以便保证编码框旋转4次后，方框中的所有小格都显露过，并且不两次显露呢？设计编码框，有一种简单的方法，我以一个横竖为6格的方框演示它。36个格中，有9个被剪掉。如图8.2左边所示，我们将编码框分成4个分框，每个框横竖为3格。我们为第一个小框中的9个格，依次从1至9排号，然后进行3次90度旋转，每次都以同样方式为左上部的分框编号，这样在大方框中最终并列着4组1至9。现在选9个格剪掉。我们从排号为1的4个小格中挑出一个，然后再找一个编号2的格，接下来是编号为3的，以此类推，直至有9个格被标明。我们共有262144种标注方法可供选择。剪掉标出的格。每个可能形成的编码框旋转4次，每个格都会精确地显露一次。如果我们想制作一个横竖8格的编码框，同样可以进行相应的操作。这时4个分框的大小都是横竖4格。然后会有16个格从编码框中被剪掉。

1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1

		3		4	
		6			2
	8				
	9				7
				5	
1					

图8.2：如何自己制作弗莱斯纳编码框。左面：在横竖6格的正方框中，人们将数字从1至9依次填入左上面的分框中。然后按顺时针方向旋转90度，再把数字1至9写入左上面的分框中。这样进行下去，直至36个格被占满，这时方框看上去正如左边的图。在正文中可以看到如何确定应被剪掉的小格（右边的分图）。

这种所谓的“转框法”几乎不会给窃码者制造什么困难。我们已经注意到，密文的长度能让人确定编码框的大小，以及

给我们如何得到确认被剪格的提示。虽然有这样那样的缺点,在第二次世界大战中,编码框还是被南美的德国间谍用来同德国反间谍机构进行电报通讯。

密钥词置换

正如我们在桑道夫伯爵的例子中已看到的那样,转框法的弱点在于编码框,它必须进行交换,因而易落入他人之手。还有另外一些方法,也是通过置换为明文加密的,而且不需要使用容易泄密的编码框。

让我们再次给桑道夫伯爵的情报加密。首先,我们将明文写入一个长方框内,不设字间距,每行 15 个字符,如图 8.3

a l l e s i s t b e r e i t b

e i m e r s t e n z e i c h e

n d a s s i e u n s v o n t r

i e s t s e n d e n w e r d e

n e r h e b e n s i c h a l l

e f u e r d i e u n a b h a e

n g i g k e i t u n g a r n s

图 8.3:一篇写成长方形的明文。

所示。如果文本填完,长方框内还剩有空位,我们就随意补入字母。最简单的加密法应该是这样的,我们根据某项规律调换纵列,然后由上至下读每一列,并写成 7 行。但到底应根据什么规则调换呢? 调换规则正是这种加密法的密钥,发送和接收双方都必须知道它。“互换第一和第五列,以及第二和第十二列……”此类规则会比真正的情报本身还长。但有一种简单的帮助办法。我们随便选一个容易记住的句子,像“Auf

der gruenen Wiese…(在绿色的草地上)”之类。它所包含的字母数量,至少要和长方形的列数相同。然后写下提示句,并不设字间距:AUFDERGRUENENWIESE。接下来按照字母表顺序,依次对字母作统计。我们由左至右,给句子多次出现的字母编号。A 是 1 号,B 和 C 没有出现过,D 得到编号 2,3 个 E 各为 3、4、5。F 只出现一次,被编为 6 号,以此类推,结果为:

A	*U*	*F*	*D*	*E*	*R*	*G*	*R*	*U*	*E*	*N*	*E*	*N*	*W*	*I*
1	13	6	2	3	11	7	12	14	4	9	5	10	15	8

我们再把长方框置于其下,如图8.4上面部分所示。现在我

A	*U*	*F*	*D*	*E*	*R*	*G*	*R*	*U*	*E*	*N*	*E*	*N*	*W*	*I*
1	13	6	2	3	11	7	12	14	4	9	5	10	15	8
a	l	l	e	s	i	s	t	b	e	r	e	i	t	b
e	i	m	e	r	s	t	e	n	z	e	i	c	h	e
n	d	a	s	s	i	e	u	n	s	v	o	n	t	r
i	e	s	t	s	e	n	d	e	n	w	e	r	d	e
n	e	r	h	e	b	e	n	s	i	c	h	a	l	l
e	f	u	e	r	d	i	e	u	n	a	b	h	a	e
n	g	i	g	k	e	i	t	u	n	g	a	r	n	s

a	e	s	e	e	l	s	b	r	i	i	t	l	b	t
e	e	r	z	i	m	t	e	e	c	s	e	i	n	h
n	s	s	s	o	a	e	r	v	n	i	u	d	n	t
i	t	s	n	e	s	n	e	w	r	e	d	e	e	d
n	h	e	i	h	r	e	l	c	a	b	n	e	s	l
e	e	r	n	b	u	i	e	a	h	d	e	f	u	a
n	g	k	n	a	i	i	s	g	r	e	t	g	u	n

AENINEN EESTHEG SRSSERK EZSNINN EIOEHBA LMASRUI
STENELL BERELES REVWCAG ICNRAHR ISIEBDE TEUDNET
LIDEEFG BNNESUU THTDLAN

图 8.4:为图 8.3 中的明文加密。上面部分:借助密钥(AUFDERGRUENENWI)为纵列编号,并作相应排列(中间)。下面部分:通过按纵列读字母,产生密文。这相对而言较易被破译。

们按数字顺序调整纵列，得到图 8.4 中间的顺序。然后以纵列为单位，将字母写为 7 个一组，就得到了图下部的密文。

接收者已知道密钥，即关于绿色草地的那个句子，他通过清点，列出数字序列：

1 13 6 2 3 11 7 12 14 4 9 5 10 15 8

然后他把第一个 7 字组作为一列，写到数字 1 下面，第二个 7 字组归到数字 2 下面，以此类推。这样，在他面前的横行中就产生了明文。运用这种方法，只须交换密钥绿色草地，而不需要编码框。

不过这种加密法也不是特别安全。窃密者可以从密符的数量和分组中推断出长方框中的长和宽，并列出一张表，如图 8.4 下面部分的长方框。在长方框中，字母 C 共出现两次，一次在第二行，一次在第五行。第二行中除了一个 H，德语中的 C 后面就没有别的字母了，于是可以推断，第十列一定位于第十五列之前。而对于第五行中的 C，H 似乎位于第二和第五列中。于是其中一列很可能紧跟在第九列之后。脱密者对两种可能性，都必须尝试。我们知道是第五列。然后他可能致力于寻找出现频率最高的字母组 ei 和 ie，或搞清纵列的交换，以得到 en。为了简化工作，他可以将每一列写到一张纸条上，尝试不同的位置交换，观察是否有意义的文章片段出现。

这种加密法的优点在于，可以轻易改变密钥。例如，第二次世界大战中驻巴西的德国间谍网络负责人约瑟夫·施塔齐克茨尼，就采用上述方法同汉堡的反间谍机构进行密码联络。他所使用的密钥选自一本西班牙语书。按照事先同汉堡约定的规则，他根据当时的日期，计算出当天使用的页码，然后打

开这一页，先用前20行的头一个字母作为密钥文，就像我们选用的“绿色草地”那句。像我们一样，他也得出一串数字，然后根据这个数串，调换已写入长方框内的明文纵列。接收者的手边当然放着同一本书。他也根据日期算出页码，确定20个密钥字母。虽然密钥每天都变化，但美国人依然没费多大周折，就解读了加密情报。[①]

我们不妨再前进一步，在对调纵列之后，对横行也进行同样操作，即采用重叠加密法。在目前情况下，我们需要一个不少于7个字母的提示词，如“Kalbsbraten”(烤牛犊)。我们为前面七个字母编号：

K	*A*	*L*	*B*	*S*	*B*	*R*
4	1	5	2	7	3	6

然后据此对已用“绿色草地”加密的文本进行横行移位操作(图8.5)。现在我们按列归成7字一组：EIEANNN ETEESGHRSRSSKE…。现在除绿色草地之外，Kalbsbraten也需被作为密钥词进行置换。我们借助第二个密钥词得不到许多东西；人们还是可以利用常见的字母对，正确排列密文纵列。这样，每一横行中都提供了明文的一部分，我们只需再将横行换位，这不会带来什么困难。不管怎么说，对一篇已通过一种置换加密过的文本，再按照移位法进行重叠加密，的确会令窃码者的日子更难过。整个过程为先是打乱字母表(置换)，然后再打乱文本(移位)。

在这方面，有一种波利比乌斯式的置换加密法可供参考，

---

① F·布拉策尔，L·B·劳特，“南美的反间谍密码”，《密码学》，1983年4月，第132页。

其中每个明文字母都对应一个数字对。虽然这只是单码加密,只需简单的频率分析就可脱密。但如果我们把由此得来的文本,再用移位法随意编排,那么数字对被拆散,也就不能进行频率分析。因为对应 e 的数字对 51,分处于两列中,而且会在随后的移位中被拆开。

*K*4:	a	e	s	e	e	l	s	b	r	i	i	t	l	b	t
*A*1:	e	e	r	z	i	m	t	e	e	c	s	e	i	n	h
*L*5:	n	s	s	s	o	a	e	r	v	n	i	u	d	n	t
*B*2:	i	t	s	n	e	s	n	e	w	r	e	d	e	e	d
*S*7:	n	h	e	i	h	r	e	l	c	a	b	n	e	s	l
*B*3:	e	e	r	n	b	u	i	e	a	h	d	e	f	u	a
*R*6:	n	g	k	n	a	i	i	s	g	r	e	t	g	u	n

*A*1:	e	e	r	z	i	m	t	e	e	c	s	e	i	n	h
*B*2:	i	t	s	n	e	s	n	e	w	r	e	d	e	e	d
*B*3:	e	e	r	n	b	u	i	e	a	h	d	e	f	u	a
*K*4:	a	e	s	e	e	l	s	b	r	i	i	t	l	b	t
*L*5:	n	s	s	s	o	a	e	r	v	n	i	u	d	n	t
*R*6:	n	g	k	n	a	i	i	s	g	r	e	t	g	u	n
*S*7:	n	h	e	i	h	r	e	l	c	a	b	n	e	s	l

EIEANNN ETEESGH RSRSSKE ZNNESNI IEBEOAH MSULAIR TNISEIE EEEBRSL EWARVGC CRHINRA SEDIIEB EDETUTN IEFLDGE NEUBNUS HDATTNL

图 8.5:在图 8.4 中间的分格中,利用提示词"Kalbsbraten"进行重新编号、排序(中间),然后按纵列读出密文(下面部分)。

比如,我们可以把一篇用图 7.2 密钥表改写成数对形式的文本,归入正方框内,再选用自己的提示词,调换纵列,再按列写出密文。

第一次世界大战中的波利比乌斯加密法

1918 年 3 月 5 日，监听德国无线电通讯的法国报务员，陷入一片恐慌。因为突然间，所有的无线电讯只由 5 个不同的字母排列组成。莫尔斯电码的长短音仅发出单调的 A、D、F、G 和 X。由耳机中记录下来的电讯，都类似 AGXXDD AG-GFD AADXFX AGFGXD AAXAG，报务员们一下子反应过来，为什么恰恰总是这几个字母反复出现，因为它们最容易相互区别。他们又进一步发觉，所有电讯的字符总数都是偶数。

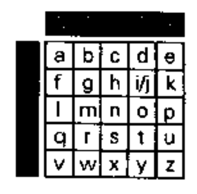


图 8.6：一张在第一次世界大战中使用的用于 ADFGX 系统的波利比乌斯密表。

德国人忽然在整个西线启用新的密码系统，这一做法令人们怀疑，一场策划已久的德军大规模进攻就要展开了。事实上它该在 1918 年 3 月 21 日在索姆河畔发动进攻。于是，弄清德国电台目前使用的密码系统，迫在眉睫。

这是一种带有移位的波利比乌斯加密法。它以下面的表格为基础将字母表中的 25 个字母（不分 i 和 j），按照图 7.2 的方式，写入一份波利比乌斯表。但不同的是，这次我们采用字母 A、D、F、G 和 X 为行和列命名（图 8.6）。我们不一定非要按字母表顺序填写表格，可以使用一个密钥字，如图 7.2 下表所示。为了方便，表中保持了字母表顺序。现在我们找一

篇简单的明文,并写成5字一组,如图8.7上面部分所示。借助图8.6中的表,我们得到了第一份(单码)密文(图8.7左下)。如果隐去字间距,就得到了一个如图右下所示的方框。我们只取密钥字“KALBSBRATEN”的前10个字母,如图8.8所示,调换纵列,按纵列读出,于是产生了图8.8下的密文。这样,方框被再一次加密。

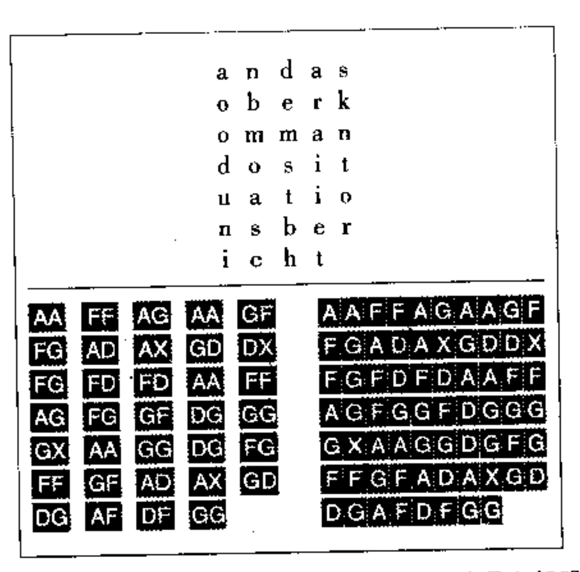


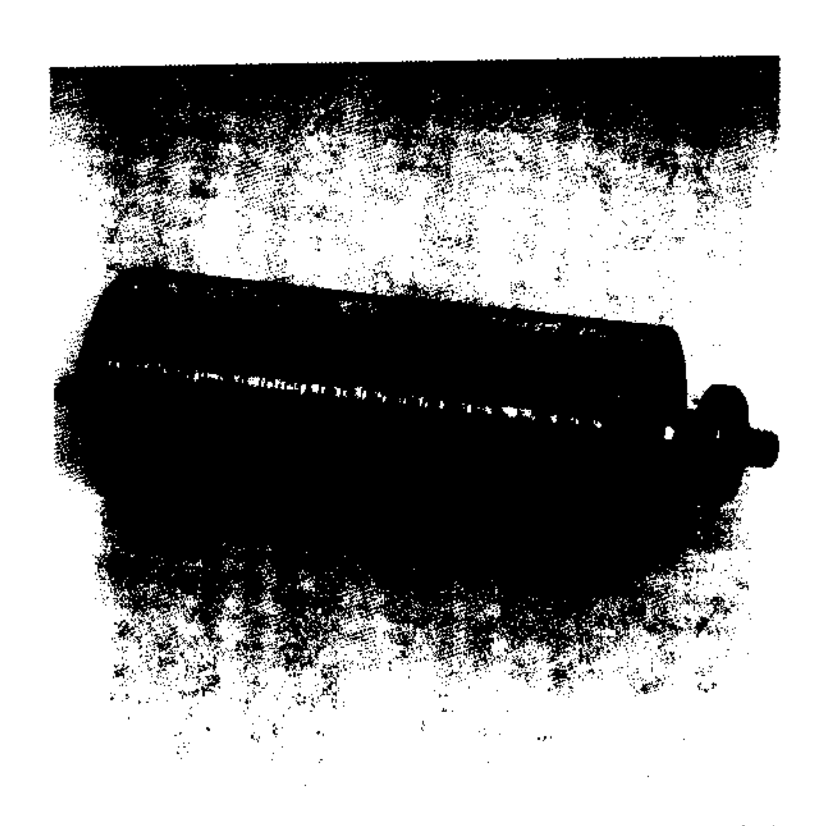
图8.7 上部:一篇明文,每行有5个字母。下部:左边是上部明文的单个字母,已经根据图8.6的乱码表,用ADFGX系统的字母对进行置换。右边是隐去字间距的相同部分。

K	*A*	*L*	*B*	*S*	*B*	*R*	*A*	*T*	*E*
6	1	7	3	9	4	8	2	10	5
A	A	F	F	A	G	A	A	G	F
F	G	A	D	A	X	G	D	D	X
F	G	F	D	F	D	A	A	F	F
A	G	F	G	G	F	D	G	G	G
G	X	A	A	G	G	D	G	F	G
F	F	G	F	A	D	A	X	G	D
D	G	A	F	D	F	G	G		

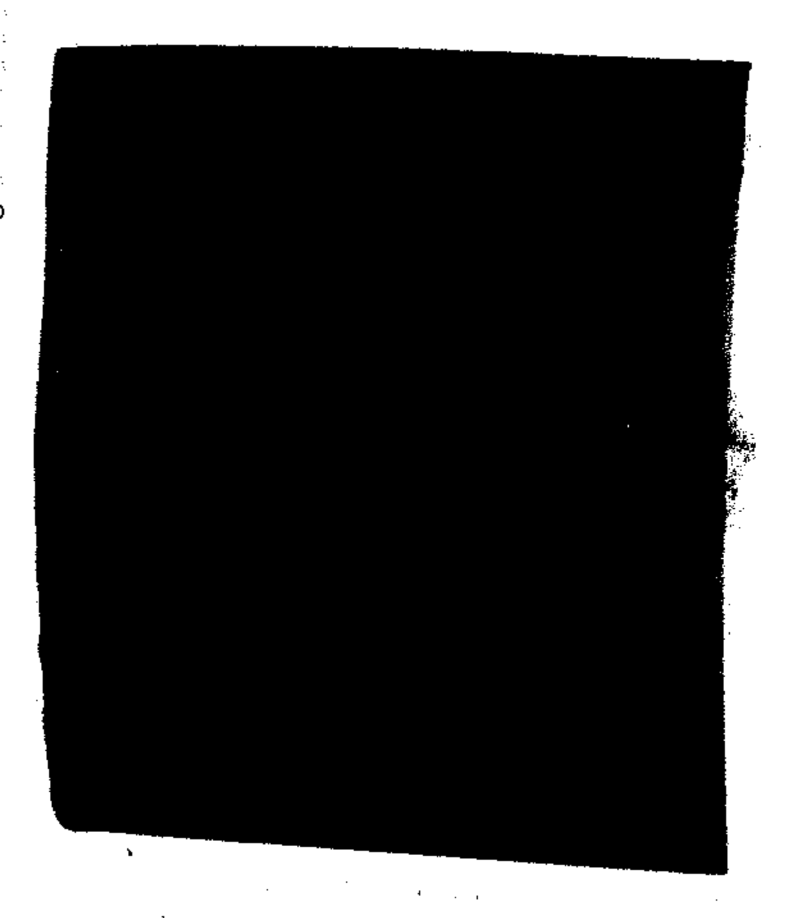
1	2	3	4	5	6	7	8	9	10
A	A	F	G	F	A	F	A	A	G
G	D	D	X	X	F	A	G	A	D
G	A	D	D	F	F	F	A	F	F
G	G	G	F	G	A	F	D	G	G
X	G	A	G	G	G	A	D	G	F
F	X	F	D	D	F	G	A	A	G
G	G	F	F		D	A	G	D	

AGGGXFG ADAGGXG FDDGAFF GXDFGDF
FXFGGD AFFAGFD FAFFAGA AGADDAG
AAFGGAD GDFGFG

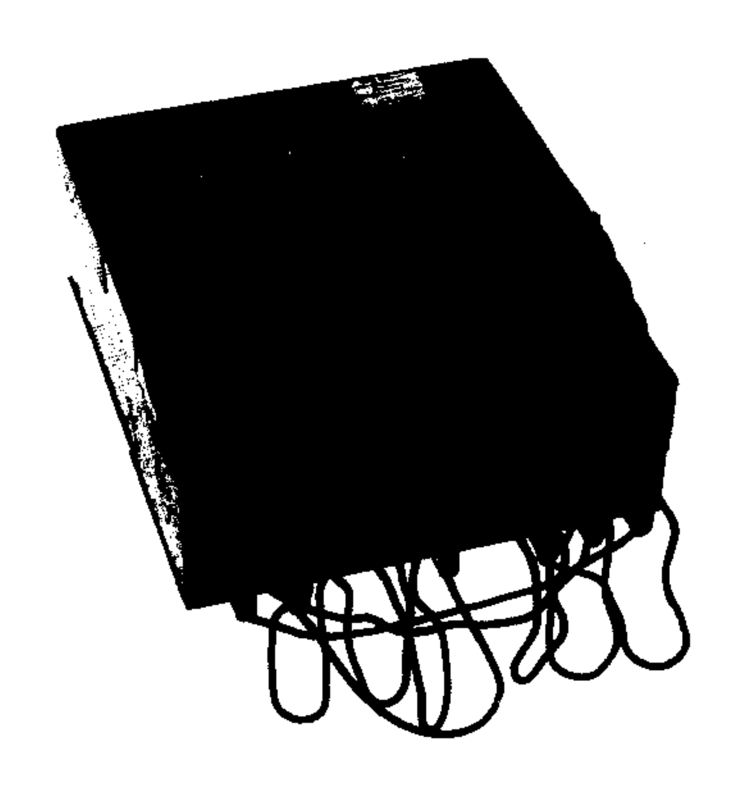
图 8.8:将图 8.7 下通过置换得到的数列,如图 8.4,借助一个提示词重新排列(中),再按列读出密文(下)。



图Ⅰ:托马斯·杰斐逊的编码轮,1920 年还被美国军队使用。不过今天,那些互相转动的密码片已不再是木制的。(图片提供:德意志博物馆)



图Ⅱ:一张苏联秘密机构使用的随机数表。在这个表中,原书166页中提及的缺点显然已被克服,因为有大量的数字重复出现,甚至有3次连写。(图片提供:密码学协会,楚格)



图Ⅲ:1944 年的四密钥轮式"马林—恩尼格玛"机。明文字母打入打字机键盘。每键人一个字母,密码字母携带的玻璃片后的灯就会闪亮。脱密以相同方式进行,键人密码字母时,会闪现出明文字母。"恩尼格玛"机开始工作之前,得预先设定好当天的密钥。也就是说,加密者要将密钥轮按正确的行序和正确的环形位置置入机器。他必须把带有滚花板的密钥轮设置好,以便指定的当日密钥能在视窗中显现。最后,还得在插塞板上(前面)插上正确的联接线。(图片提供:德意志博物馆)

图Ⅳ:"恩尼格玛"机的两个变码旋转件。左:密钥轮Ⅰ。可以看到滚花轮和齿轮。在加密时,滚花板通过齿轮转动。销钉的作用是作为接触点,接触下面一个密钥轮上的触点表面。右:密钥轮Ⅷ的放置,便于看清26个圆形接触面和与此相关的调节环上的字母。在调节环上还可看到两个缺口,通过它们可带动下个密钥轮的转动。其带有电路接触点和配线的内部,相对于滚花板、调节环和销钉组成的外部,也是可以转动的。就此调节当日密钥中规定的密钥轮环形位置。(图片提供:德意志博物馆)

破译者反其道而行之。他将横行写成纵列，因为他知道，这是由 KALBSBRATEN 调换而来的，他可以再逆向操作调换。这样，他借助波利比乌斯密表从字母对进人明文字母。对于密钥，他只需知道 KALBSBRATEN，倘若波利比乌斯密表是借助一个密钥词填写的，正如这个。

当法国的密码专家乔治·潘万还在为无法解读的无线电讯绞尽脑汁时，德国人距巴黎城门只有约 50 公里了。然而恰在此时，他揭开了 ADFGX 无线电讯之谜，法国人又可以破译德国的无线电通讯了。可德国人早有准备，他们采用了一种新的密码，在其中在前面提到的 5 个字母外，又增加了 V。

使用这 6 个字母可以建立起一份 36 格的波利比乌斯表。事实上，当时德国人掌握的密表，不仅可以区分 i 和 j，而且还包含了 0—9 的数字，潘万在 1918 年 6 月 1 日拿到了第一份用新方法加密的情报，而到 6 月 2 日晚上，他就将其破译出来。他是一位孜孜不倦的工作者。据说，他在长达数月同德国密码学家追击较量的过程中，整整失去了 33 磅的体重。可以说正是他的工作，使德国士兵在第一次世界大战时未能漫步于香榭丽舍大街。

不是所有在两次大战中功勋卓著的密码学家，在其后的平民生活中都如潘万般辉煌。1918 年，他成为著名的经济管理人，在法国最大的化学康采恩中居最高位。不过直到晚年，他仍将破解 ADFGVX 密码之谜，视为一生中的最大成就。

在近代，纵然移位法第一眼看去极富诱惑力，但相对于置换法，它已退居二线。第一次世界大战后，机器接替了加密及脱密工作。当然，如果今天仍只能依赖纸和笔加密，比如在间谍活动中，那么还是需要结合使用移位法和置换法。1957 年，正是冷战中期，苏联间谍雷诺·海哈南叛逃到美国人一边，

供出自己用来同莫斯科联系的密码系统。此系统的代号同间谍本人一样:VIC。它的工作程序分3步。首先采用波利比乌斯表的单码置换加密原文。然后通过两次复杂的移位进行重叠加密。

9

从密码盘到“恩尼格玛”机

密钥程序即加密时遵循的法则。

密钥是不断变化的文本，在各个程序中按照此文本准备为密钥介质加密。

密表即一段较长时期内使用的单个密钥的汇编。

密钥介质是加密时必需的辅助工具，如密钥机（至今被称为密码机）。

标志组是用于注明一条无线电讯中使用的密钥。

摘自秘密的《“恩尼格玛”密码机的密钥指南》，柏林，1940年

1943年5月11日，528号潜水艇的耐压艇体钢板出现裂缝，《弗利特伍德》号发射的深水炸弹与飞机投掷的炸弹在近距离爆炸，在气体逸出、浮力减弱的同时，潜艇下沉。指挥官格奥尔格·冯·拉贝瑙中尉下令鼓风，气体将海水排出潜水舱，潜水艇再次浮向水面。指挥官让话务员发出一份加密无线电

报:“潜艇失去潜水功能”。英国的反潜快艇投掷出深水炸弹后已离开作战现场。《弗利特伍德》号再次追随它的OS47运输船队。快艇战士发觉露出水面的潜艇,减速行进并开火射击。冯·拉贝瑙决定沉没528潜艇。海面上刮着中级海浪,一艘救生艇被放出,许多着救生衣的船员跳出潜艇,事先已预料到这种情况的发生并已作好准备不让加密系统落入敌军之手。当日密钥表是用水溶性颜料印在一种吸墨水纸上。不仅如此。另一个秘密就是“恩尼格玛”密码机轮子的接线方法,它也必须一同消失,话务员已取出轮子并塞入包内。

预备役少尉赖马尔·吕斯特使劲把包扔出船舷,它啪的一声落入水中,他盯着包直至看不见为止。自此,528潜艇上的“恩尼格玛”的密钥轮静静躺在爱尔兰岛西南方,北纬46°55′,西经14°44′,320米深的大西洋海底。

56名船员中有45人顺利搭上英国船只。[①]

轮子的发明

在密码学发展过程中,密钥轮直至现代还发挥着重要作用。图4.2中以二十六个区段占有两个轮盘,即“轮子”。人们将轮子相互旋转就产生“凯撒式的编密方法”。

让我们再次观察图4.10上方的电动密码机。弯曲已接线的条带使上下两窄面相互接触。条带由此形成一个圆柱体,如图9.1中间所示,把它和两个侧面连在一起形成一个插

① 战后,格奥尔格·冯·拉贝瑙中尉在联邦海军中任副舰长一职。海军少尉赖马尔·吕斯特后来成为马克斯—普朗克学会主席,如今是亚历山大·冯·洪堡基金会主席。在此六年中,他领导欧洲宇航局(ESA)。

座。图中可见此时接触点的位置。老式的接线通过插座内部相连，条带就变成一个所谓的密钥轮。通向机器开关和指示灯的接触点相应在圆圈上，轮子左边的每个接触点与一个白炽灯相接，右侧的每个接触点与开关相接，接触点排列在圆圈上，对加密没有任何影响。目前新式密码机并不比老式的密码机销售得多。其优点在于密码机的轮子可以旋转，每转1/4周，开关接触点和其他指示灯接触点相接，而轮子内部接线方式保持不变(图9.2)。

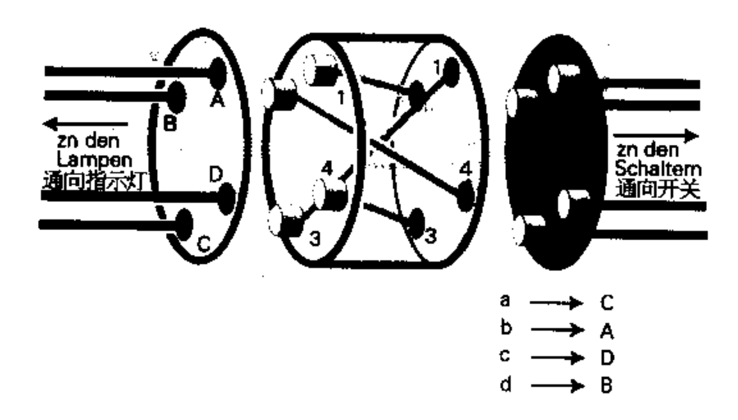


图9.1:图4.10的电路。接线已不是处于一块平面条带上，而是接在密钥轮环形插塞内部，此处省去连接电池装置。两个轮盘上载有通向开关和指示灯的接触点。这儿的电路同样如图4.10上所示把明文转换为密文。

在此，我介绍了仅带有4个字母的字母表式密码机。就正常的字母表而言则需要配备26个开关、26个指示灯，密钥轮每侧需有26个接触点，左侧每个接触点和右侧的一个相连。为避免出现单码密码，轮子的位置不能固定不变，人们可以将其稍许改变一下，每键入一个字母，密钥轮旋转1/26周。由此产生的密码和维吉尼亚密码并无本质区别。在此的每个

字母都需配备一个单码密码。维吉尼亚密码中密钥字长度决定每隔多少字母密码自动循环，我们装有密钥轮的机器旋转一周，即前进 26 位后，也为一个周期。

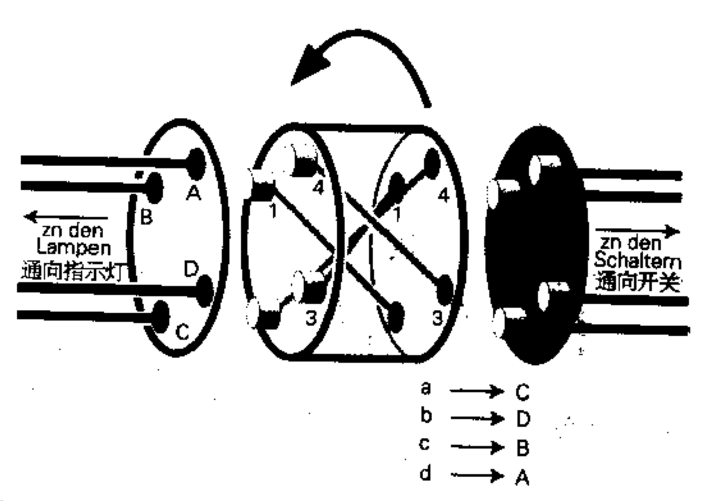


图 9.2：与图 9.1 相比，此处密钥轮沿箭头方向旋转 1/4 周，位置改变。此时开关和指示灯的连接方式也不一样，不同于图 9.1，明文字母转换为另一种密文字母。

由此得出，用我们机器产生的密码和维吉尼亚密码破译方式相同。因此这种机器并无很大价值。但密钥轮使密码艺术出现一个转折点。

三位发明家——只有一人致富

美国人爱德华·休戈·赫贝恩(1869—1952)首次成功地在技术上实现轮子原理。他把两台电动打字机——最初的模型才进入市场——相接，其中一台的键盘和另一台的操纵杆相连。稍微改动接线方式就可以产生不同的单码密码。此时是

1915年。赫贝恩1917年的简图已阐明轮子原理。运用一个轮子至多产生26个单码密码。与固定的开关和白炽灯接触点相比，这些单码密码对应密钥轮的26个不同的位置。如并列安装两个轮子，则另当别论。通过第一个轮子右侧一个接触点产生的电流经过接线导向轮子左侧的接触点，流向第二个轮子右侧接触点。图9.3所示即为简单的四字母字母表的两个密钥轮电路，只要轮子不移位，它们就只会产生单码密码。根据正常的字母表，一个密钥轮相对于另一个有26种不同排列方式，而将两轮作为一整体，与外部固定的接触点相比又有26种不同方式，由此出现26×26=676种不同位置。每按一次键输入一个字母，第一个轮子要进一位，第二个轮子则待第一个轮子循环一周后再进一位。因此在密码中每隔676个字母循环一次，这符合密钥绦虫长度为676的维吉尼亚密码。

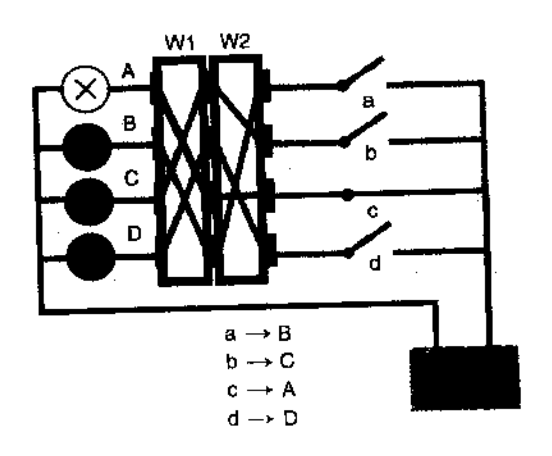


图9.3：装有两个密钥轮的电路，他们可以彼此相对并且对着开关和指示灯接触点方向旋转。与图9.1和图9.2不同，在此从侧面精确标出密钥轮。由于密钥轮彼此间的位置以及与开关、指示灯相对位置不同，在一个4字母的字母表中可有16种不同的加密方法。

企图以不正当的方式破译密码不必等待绦虫重复，只要拥有大量消息便可。只要对每条消息加密都是以密钥轮处于同一起始位置开始的，所有消息第一个字母均以相同方式单码加密（所有第二个字母和第三个字母等等都一样）。通过对密文字母的频率分析就可以破译单码密码，在具有大量秘密无线电文的情况下不仅可以复原明文，而且还能弄清两轮的接线方式。只有当各轮子之间以及轮子和固定接触点之间的起始位置根据不同的消息经常变动时，这种方法才无法奏效。

赫贝恩的第一台机器装有5个轮子。它就有 $26\times26\times26\times26\times26=11881376$ 种不同的调节方法（图9.4）。

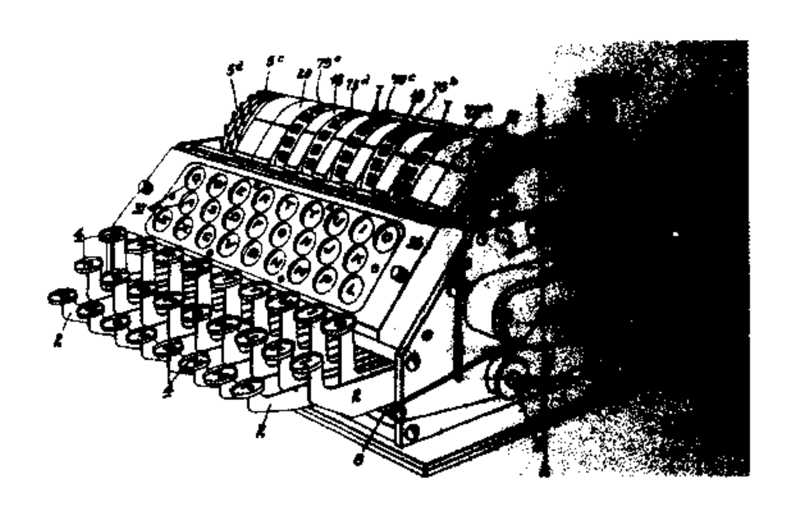


图9.4：赫贝恩的电动密码机示意图（1921年）。

赫贝恩作为发明家是天才的，作为商人是不走运的。1921年，他在美国创建首家密码机公司。他坚信自己的发明将开辟密码的新纪元，他的想法不无道理，他发行股票并在加

利福尼亚州的奥克兰市建立一家大型工厂。美国海军部对他的机器感兴趣,他希望他们将大量购买自己的机器,这是个错误。1924 年至 1926 年间,公司总共收到两份订单;一家私营公司,意大利和英国海军总共购买了 9 台。价格为几百美元。每股以 5 美元发行的股票跌至 1 美元。赫贝恩的公司陷于破产的境地。

在第二次世界大战及以后的冷战期间,美国军方使用了数十万台密码机。它们都是根据赫贝恩轮子原理工作的。经过一场旷日持久的诉讼,他得到 3 万美元的补偿,这并非是为了满足他的申诉要求,而是为了尽快了结这场诉讼,因为军方的密码秘密可能被公开。此时,赫贝恩已去世 6 年。

赫贝恩并不是密钥轮的唯一发明者。1919 年 10 月,来自德尔夫特的许戈·亚历山大·科赫在荷兰申报"密码机"的发明专利权。1927 年,他把此专利权转让给一位德国工程师,阿图尔·舍尔比乌斯(1878—1929)。此人于 1918 年就已在德国申报一项根据轮子原理工作的密码机专利权。舍尔比乌斯不仅得到密码机构思的专利权,而且还制造机器。密码机的具体细节可从他在美国的专利申请中一见端倪(图 9.5)。这种机器的另一特别之处即为互动轮。在插图最右端可见用数字 11 标明的互动轮。

在舍尔比乌斯式机器中,每打一个字母,轮子就移动一位,循环一周后,下一个轮子也移动一位。通过具有不同传动比的一种传动装置,其他轮子也在每个字母后移动一定位数。

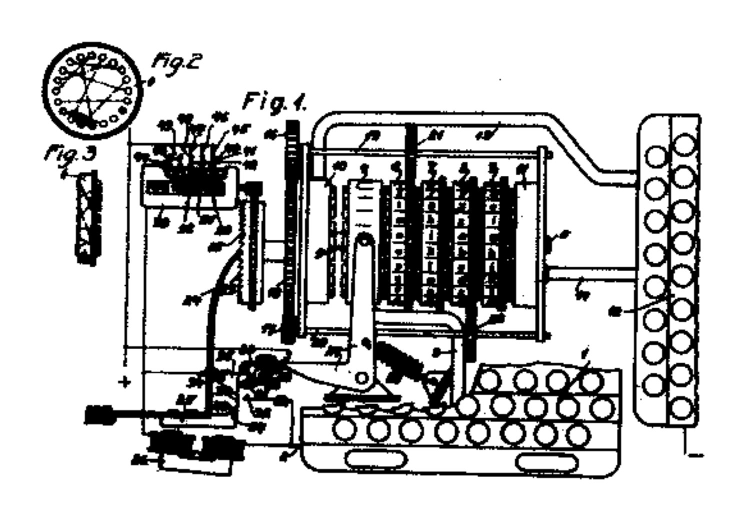


图 9.5：舍尔比乌斯式机器示意图。左上方是已接线的密钥轮（1923年）。

图 9.6 描述了电路原理。这是配有两个活动式密钥轮机器的示意图。最右端是(不可转动的)互动轮，在标出的轮子位置按 c 键，B 指示灯亮。马上可以看到，按 b 键则 C 灯亮。这便是互动轮带来的优点：使用同一台机器既可加密也可脱密。如果密钥轮居于某一特定起始位置，依次键入一段明文字母“adac”，当密钥轮逐渐旋转的同时，DCBA 灯依次闪亮。如果此时密钥轮起始位置不变，键入明文字母“dcba”，则指示灯 ADAC 亮，明文又出现了。因为脱密时，输入每一字母，密钥轮相对的位置和加密时都一样。如在图 9.6 中所见，每个这样的电路中的明文字母和密文字母不可能相同。

谁想用这台机器破译加密的消息，不仅需了解各个轮子的接线关系，而且还需知晓它们在机器内是以什么顺序排列的。除此之外还要了解互动轮的接线关系以及密钥轮相互间转动的规律。

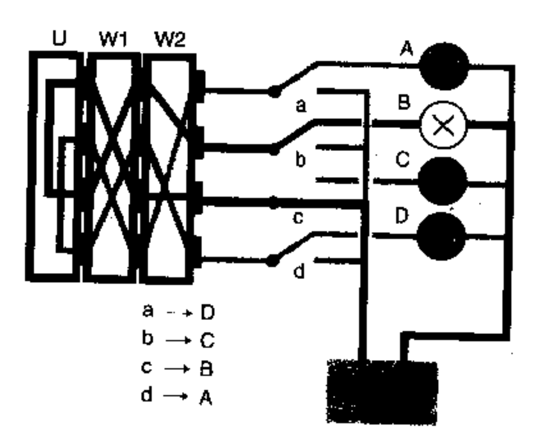


图 9.6:图 9.3 的两轮密码机加上一个互动轮(u)。加密的同时,轮 W1 和 W2 移动,而互动轮静止不动。键入一个明文字母,相应字母的指示灯决不闪烁。如图示,合上开关 C,与此同时指向 C 灯的电路立即中断。

舍尔比乌斯把这台机器命名为"恩尼格玛",希望促进它的销售。希腊语"恩尼格玛"(Enigma)是谜语之意。他制造了许多型号不同的机器并于 1923 年成立一家股份公司。同年 8 月,坐落在柏林市施特格利茨大街的公司开始投产。舍尔比乌斯在专业大会上展示他的"恩尼格玛",但却未达到预期的商业效果。

但这种机器引起德国国防军密码机构的兴趣,依据《凡尔赛条约》协约国允许德国拥有 10 万陆军。尔后,这种机器不再为商业,而仅仅只为军事生产。

1934 年公司解散。3 年后,舍尔比乌斯在一次车祸中丧生。当希特勒上台执政并开始扩充军备之际,"恩尼格玛"获得新生。以后我还将详细介绍"恩尼格玛"在第二次世界大战中所起的作用。此处言归正传,回到密钥轮原理发明者议题上来,还有第三位发明家。

1919年10月,科赫在荷兰申请专利权的3天后,瑞典人阿维·热拉尔·达姆在斯德哥尔摩申请专利权。今天人们宁愿称他为技术怪才。他原是芬兰一家纺织厂的工程师,他对厂里的织布机进行多项改进,他在家中能通过写字台上的按钮打开门并开亮电灯。就私生活而言,他并不是循规蹈矩的人,据说他曾骗取一个作风正派的马术女演员的芳心,与她举行结婚仪式,而婚礼上的牧师则是由一位朋友乔装打扮的。

第一次世界大战爆发后,达姆和一位英国纺织工业主在德国专利局替密码机申请了3项专利权。令人惊讶的是在德国,他的合伙经营人在那里被视为敌人。后来他创建了一家公司,为此他当然需要资金。他迅速找到投资商阿尔弗雷德·诺贝尔,这位甘油炸药的发明者和以他名字命名的诺贝尔奖的设立人,他的侄子也是投资人之一。这位拥有显赫亲戚关系的投资者又拉了另一位叫哈格林的赞助者。

达姆制造了许多台机器并向潜在的客户展示。它们并未成为畅销货。图9.7所示的是1922年公司目录的扉页。后来,一位新人加盟这项计划:鲍里斯·凯撒·威廉·哈格林,他是前面提到的一位合伙人的儿子。小哈格林是位工程师,并在俄罗斯、瑞典和美国积累了工作经验。此时他简化了一台达姆式机器,装上一个键盘以及赫贝恩式机器的指示灯。1929年,他成功地售出了大量这样的密码机。当达姆于1927年去世时,哈格林接管了公司并继续改进型号。1934年,他启用打点式记录器以替代指示灯。他的机器虽然一直是37磅重,但能塞进公文箱内,并且一分钟内能译200个字母。法国总参谋部询问哈格林能否把机器连同记录器改装成只有口袋般大小。纪录很重要,因为使用指示灯时,如果需要快速加密或脱密,第二个人得在场。哈格林成功地把机器改装为低于3

磅重，机体比当时使用的电话机还小。后来他卖给法国人3500台这种型号的密码机。



AKTIEBOLAGET
CRYPTOGRAPH
STOCKHOLM . SWEDEN

MAKERS OF
CIPHERING MACHINES OF ALL KINDS
FOR DIPLOMATIC MILITARY AND MARINE SERVICE AND TELEGRAPHIC AND COMMERCIAL CORRESPONDENCE

CONSULTANTS FOR
ALL CRYPTOGRAPHIC MATTERS

图9.7:1922年密码机公司的扉页。当时的老板还是发明家阿维·热拉尔·达姆。10年后，鲍里斯·哈格林接管这家公司。

1904年，当德军的铁蹄践踏挪威时，哈格林担心瑞典不再安全。他决定退却去美国。在此期间，希特勒占领了法国、荷兰和比利时。再也没有商船从挪威驶往美国。因此哈格林一家想出一个冒险计划，在热那亚上船。他们从特雷勒堡出发经柏林横穿希特勒统治下的德国。3天后，他们抵达热那亚，搭乘“康特·迪·萨瓦亚”号到达纽约，并且随身携带了密码机设计图纸。在美国，哈格林还成功地从斯德哥尔摩把50台机器运入纽约。他在美国立即生产。他的机器优点在于5个轮子不规则旋转，致使大约出现一亿个字母后密码才会重复。第二次世界大战期间，他总共销售出14万台机器。这使他成为拥有百万美元的富翁。

战争结束前一年，富甲一方的鲍里斯·哈格林重返瑞典，并在斯德哥尔摩南部设立工厂。第二次世界大战后，他的生意如日中天。战后国际关系重组过程中，新兴的国家需要大量密码机以应军队和使馆联系之用。哈格林了解瑞典的法律准许把有益于国防的发明收为国有。这项法律，尤其是瑞典的税额促使他在 1948 年把发展部门迁往瑞士的楚格州。大约 10 年后，整个公司移往瑞士，在那里最终有 170 名工人从事密码机的生产。1959 年，这位唯一通过发明密码机致富的鲍里斯·哈格林离开人世。他的密码机有限公司仍在楚格州。公司的目录表明产品销往 130 个国家，其中也包括伊拉克、伊朗和利比亚。

互动轮的灾难

正如我们所知，舍尔比乌斯式机器的互动轮的优点在于能使用同样的机器加密和脱密。第二次世界大战中德国人并不了解互动轮与生俱来的严重缺点。以后我们将看到，正是互动轮使得波兰和英国的密码学家能够破译由“恩尼格玛”加密的信息。

使用同样的机器加密和脱密，加密的可能性受到极大限制。我们知道轮子的每个位置与一个开关和一个白炽灯相连。由于开关和指示灯都用字母标出，这也意味着机器给每个明文字母配备了另一密文字母。我们就可以对字母表进行置换、随意组合或排列。装有互动轮的机器极大地限制了可能的密码数目。它仅利用排列，两次使用字母表，它们又重复了原先的秩序。如下借用四字母表的例子阐述这一道理。

使自己毁灭的排列

在四字母表的简单情况下存在 24 种排列，即：

ABCD	ABCD	ABCD	ABCD	ABCD	ABCD
ABCD	ABDC	ACBD	ACDB	ADBC	ADCB
ABCD	ABCD	ABCD	ABCD	ABCD	ABCD
BACD	BADC	BCAD	BCDA	BDAC	BDCA
ABCD	ABCD	ABCD	ABCD	ABCD	ABCD
CBAD	CBDA	CABD	CADB	CDBA	CDAB
ABCD	ABCD	ABCD	ABCD	ABCD	ABCD
DBCA	DBAC	DCBA	DCAB	DABC	DACB

但是只有三种排列在第二次使用中有把每个字母换为自身的特点。即：

ABCD	ABCD	ABCD
DCBA	CDAB	BACD

我们来验证。看第一组。它使 D 代替 A，但也让 A 代替 D。第二组中 C 替代 A 而 A 也代替了 C。但也让 D 替代 B，B 也代替了 D。第三组亦如此：我们可以用一种排列，比如用第一组加密整段文本。明文 ADAC 的密文为 DADB。再用第一组排列加密 DADB 得到 ADAC——又是这样。两次加密显现明文。在排列的语言中（比较原文 94/95 页的方框）我们可以说：启用装有互动轮的"恩尼格玛"产生的排列使得每一个字母都有自己的倒数，即反排列。第一次排列产生的效果在第二次使用时被抹去了。数学家称诸如此类的排列为对合。24 组可能的排列中只有 3 组具备这种特征。

如果我们采用 26 个全字母表，情况又将如何？在第四章中我们已讨论过，使用全字母表频率转换数目长达 27 个小数位。如果在同一状态中两次将方法运用于一篇明文，机器

1 1
3
5 5
7 7 7
8
9 9
0 0 0

会再次显现同一明文,那么这样的频率转换数目只是13个小数位。虽然这个数字仍然庞大,但它已比前一个数字缩小了几十亿倍。使用同样的机器加密和脱密,其可能性就大打折扣。

没有L的无线电报

互动轮的优点就是同样调节机器即可加密和脱密。这导致了另一后果。不管人们键入什么字母,同样字母的指示灯决不会闪烁。借用图9.6我们不难理解:此时按下某一特定字母开关,在图中是C开关,电流并非流向C灯。任何明文字母都不可能进入同一个密文字母。第二次世界大战中人们利用这一特点破译了一条无线电报,尽管其内容无聊透顶,但却使意大利海军失去了在东地中海的霸权地位。

梅维斯·利弗是伦敦大学的女学生,16岁时就加入第二次世界大战英国密码机构中心破译者的俱乐部——布雷契莱庄园。意大利海军的一份篇幅较长的无线电报全文中没出现字母L,这一情况引起她的注意。在一段密文中,如果不是单码加密或根据维吉尼亚法加密,字母表中所有字母出现的频率应大体一致。为何报文中没有出现L?梅维斯小姐心中疑窦丛生。这是否是意大利译电员玩弄的迷惑手法?他们在“恩尼格玛”机上选择字母1彼此对接作为明文,以此误导盟军。她想如果这样,密文中就不会出现L,因为1决不会转换为L。如果她估计正确,那么以此就可了解意军使用的“恩尼格玛”机的内部构造。当梅维斯小姐继续琢磨这个想法时,她发觉自己没错。密文告诉她机器在轮子按顺序转动中从1中造出什么。由此她得知它的接线方式并成功破译密码。意大

利战舰发出的无线电报使得英军于 1941 年 3 月在科林斯最南端的马塔潘角战役中一举歼灭意军的 3 艘巡洋舰和 2 艘驱逐舰，这次打击使意大利海军从此一蹶不振。[①]

不过在有意义的无线电报中，在一般电文中，装有互动轮的“恩尼格玛”机的缺点也引人注目。所有互换的数目经过两次使用重现原来的规定，还展示了其他一些规律。它们虽无济于直接破译密码，但是启用互动轮导致可能出现的密码数量大量减少，操作中愚蠢的失误和漫不经心使得波兰数学家在 30 年代就破译出用“恩尼格玛”机加密的情报。尔后盟国由此受益。美国人在第二次世界大战中使用数以千计的哈格林密码机内就未安装互动轮。

希特勒的“恩尼格玛”机

1933 年，希特勒上台后，舍尔比乌斯式密码机几经改进。多种型号的密码机投入使用。陆军、海军和外交部启用了不同型号的密码机。但是它们最终都与 1928 年就装有插板的舍尔比乌斯式密码机雷同。插板上有 26 对双头插塞。电线从键盘开始经插塞通向轮子，回过来再与指示灯相连。这样使字母表的 26 个字母中的某些字母排列顺序再次被打乱。德国国防军启用的“恩尼格玛”机配有 3 个密钥轮、一个互动轮和一块插板。图 9.8 即为使用四字母表的示意图。

给插板接上插线产生如下顺序：

ABCDEFGHIJKLMNOPQRSTUVWXYZ
EYCFADHGOKJMLNIWQSRUTZPXBV

① D.卡恩：《抓住恩尼格玛》，波士顿，1991 年，第 86 和 139 页。

图 9.8:简单型四字母表“恩尼格玛”机示意图。开关 a、b、c、d 分别与指示灯 A、B、C、D 相连。电线从开关穿过插板 S,穿过图中用 W1、W2 和 W3 标明的 3 个密钥轮,经互动轮 U,再通过 3 个密钥轮和插板接指示灯。图中已按了开关 C、D 灯亮。密钥轮随着每个加密字母依次转动并且改变密码。可以确信,它是对合的:图中密文字母 D 亮是因为按了明文字母 C,而 C 亮则是按了 d。因此 ad ac 转换成 BC BD。bc bd 转变为 ADAC。此外可见,任何明文字母在密文字母中都不可能相同——这就是“恩尼格玛”机的一大缺陷。

注意:此处是一次互换,例如 A 转换为 E 的同时 E 也转换为 A。如果把它用于明文,再用于互换的电文,那么原先的明文就会再次显现。互换就是一种对合。

图表Ⅲ展示了实际操作。此处所示的是第二次世界大战临近尾声时,德国海军使用的四密钥轮密码机。在图表Ⅳ中可见已取出的两个密钥轮。每个密钥轮都由一个内部零件构成,它的两侧载有电子接触点,并且在内部,一侧接触点与另一侧的接触点相连。在内部零件周围连着一个圆环,这在图表Ⅳ的右侧密钥轮可以看见。它处于字母表 26 个字母的外部,另外它还有一个或两个缺口,这是拨动下一个密钥轮所需

的。如果机器内装有这个密钥轮，从机罩的窗口上就可看见圆环对着的字母，以此可以读出密钥轮所居位置。密轮上的一个滚花轮伸出机罩便于从外部就可以转动机器内的密钥轮。在适当的位置，一个圆环缺口打开一个传动装置，它在按下一个键时，也拨动下一个密钥轮向前进一个字母。图表Ⅳ下方画出的密钥轮显示，如果窗口中出现字母 E 或 M，那么下一密钥轮就移动了。

还有更为复杂的情况：缺口环和密钥轮载有接线及接触点的内部零件能够相互旋转。这就有可能改变圆环的位置，即圆环和零件相互转动。这也就增加了对方的破译难度。

第二次世界大战开始时，密钥轮增加到 8 个。它们代号为Ⅰ、Ⅱ……Ⅷ。每个密钥轮都有各自的缺口字母环。内部零件中都有各自独特的接线。在图表Ⅳ中画出左边的密钥轮Ⅰ，右边的密钥轮Ⅷ。

加密者可以对机器进行多种调节。他能做到：

1．从众多的密钥轮中选出 3 个（如果使用四密钥轮的"恩尼格玛"机，可选择 4 个）；

2．把每个密钥轮调至规定的圆环位置；

3．按一定顺序插入密钥轮（三密钥轮有 6 种插入方法，四轮则有 24 种）；

4．把 3 个密钥轮拨到起始位置，使字母窗上可见 3 个特定字母（四密钥轮亦如此）；

5．插上插塞连结。

加密者必需根据手头的当日密钥按秩序进行操作。这样他才能保证负责脱密接收电报的同事把自己的"恩尼格玛"机调至同样的起始位置。图 9.9 列出了第二次世界大战中"恩尼格玛"机的使用。



图 9.9:第二次世界大战中投人使用的"恩尼格玛"机。装甲兵将军古德里安在等待破译无线电报。(普鲁士文化遗产图片档案)

由于更换密钥轮是件费力和冒险的事，1935 年之前，德军每三个月变更一次密钥轮秩序，尔后逐月更换，从 1936 年 10 月起每日更换。第二次世界大战期间，每隔 8 小时就变动一次。

当时密钥包括密钥轮的选择及安装顺序，圆环位置，密钥轮的起始位置以及插板上的插线关系。这在陆军密码本中一一规定。加密者把机器这样装好才能输入明文。他按键输入电文的第一个字母。这使得他使劲按才行，因为他得用力拨动第一个密钥轮。但是这个密钥轮可能和第二个密钥轮前进一位所处的位置一样，有时甚至与第三个也一样。随着按键输入每个字母，接通一条电路，电流从键盘通过插板，3 个轮子向互动轮运转，从那里返回，通过 3 个密钥轮，但此时是以相反的方向，再次运转经插板直至一个指示灯。指示灯亮，脱密者按键输入第二个字母，又一指示灯亮。他必须习惯用左手按键输入明文，用右手记下密文，即灯座显示的密码。他必须把这样得到的密文交给报务员发送出去。

从报务员处收到密文的接收员必须一手按键输入密文字母，另一只手记下灯座闪亮显示的明文。

1942 年 2 月，德国海军增加了一个以希腊字母“β”命名的密钥轮；在术语中称之为“希腊密钥轮”，为了把它装入“恩尼格玛”机机罩内，必须减小它和互动轮的厚度。这样薄形的互动轮有 A 和 B 两种款式。薄型互动轮 B 把 ABCDEFGIJKMTV 这 13 个字母和其他的 13 个字母，即 YRUHQSLPXNOZW，连接在一起。

现在人们似乎有理由认为：解密者一定无法破译经过如此复杂程序加密的电文。他既不知道密钥轮的选择，也不知它们的排列顺序，既不知圆环的位置，而且对插塞连结也一无

所知，更不用说对密钥轮的接线了。

乍一看去好像没有丝毫破译密码的希望。不管当日密钥的排列如何巧妙，不管每个轮盘上有几个缺口推动下一个轮盘——按照同样的日密钥规定的秩序进行操作，每份电文的第一个字母均是以同样的机器位置加密。如果截获足量的电文，就会发觉其中有诸多的攻击点：所有第一个字母均是单码加密，第二个字母也是如此，只是与第一个不同。依次类推，不同电文中处于同一位置的所有字母都如此。所有单码加密的字母键就能依靠一种频率分析来破译。因此采用狡猾的当日密钥的最巧妙的“恩尼格玛”机最终也无济于事。

因此需要一句电文一句电文地修正调节机器。对此，一条消息的发报员必须想出一个电文密钥。它各有 3 字母构成，并且不依据当日密钥而重新确定当日密钥的起点位置。收报员当然必须知道电文密钥。怎样向他传达电文密钥而不让同时收听的敌人知道？对此，收报员可通过电文的前 3 个字母知道密钥轮新的起点位置。为此还需要使用当日密钥。如果收报员利用当日密钥译出这 3 个字母，他必须把密钥轮调整到对下面的电文有效的位置。这样他才能破译以下的密文。为确保把电文密钥的 3 个字母发送出去——密文无论如何会发送出去，但可能由于接收效果较差而到达时已面目全非，把它们发送两次，因此每份电文开头都有 6 个字母，它的明文是两个相同的三码组。由于按键输入每个字母时，轮子位置不同，因此发送的两个三码组当然不一致，而是某 6 个字母。此时收报员首先必须根据当时密钥调节密钥轮，以此对这 6 个字母脱密。如果一切正常，他应该在明文中见到两个相同的三码组。此时再根据三码组重新调节三个密钥轮位置，这样在他的“恩尼格玛”机字母窗内就出现三码组字母。

他得从这个位置出发按键输入其余的密文。

人们估计，在德国大约制造了 20 万台“恩尼格玛”机。今天只有少量留存于世。战后盟军销毁了大量的密码机。今天，“恩尼格玛”机已成为收藏品。20 年代，每台价值约为 600 马克。今天，一台原装“恩尼格玛”机市场价已升至 15 万美元。慕尼黑的德国博物馆在它的“信息和自动控制馆”里就藏有大量过去曾用于加密的机器。在那里也可见到图表Ⅲ所展示的德国海军使用的四密钥轮“恩尼格玛”机。

在附录 B 中我阐述了一个在电脑中模拟“恩尼格玛”机工作方式的程序。您的电脑将成为一台想象中的“恩尼格玛”机。您能调换密钥轮，圆环位置和密钥轮位置，确定插塞板的接线和密钥轮的起点位置。如果进行了这样的调节，您就可以随意地加密和脱密了。

1

6

9

10

揭开"恩尼格玛"机的秘密

> 历史学家……谨小慎微。但毕竟达成共识，如果没有盟军成功地破译无线电报，战争可能还会持续一至两年。这极有可能意味着在德国投掷原子弹。
>
> 赫伯特·W·弗兰克，《秘密信息》

1929年夏，24岁的波兰学生马利安·雷耶弗斯基在格廷根大学注册进入数学系学习。他来自比得哥什，他出生时这座城被称为布龙贝格，第一次世界大战后被割让给波兰。他中学毕业后在波兹南（波森）学习数学。在那里，他了解了数学的一门边缘学科。波兰参谋总部的密码机构从大学中选出20个学生开办了一个密码专修班。秘密警察把波兹南作为专修班地点是因为这座城市在1793年至1918年间属于德国领土，所以大部分学生精通德语。波兰人期望这样培养的新一代密码学家能破译德军的无线电报。当雷耶弗斯基仍在哥廷根时，他的母校向他提供助教职位。他告别德国，随后的两

年在波兹南大学任教。那儿早先的密码班并非毫无成就，甚至还设立了一个密码工作室。在那里共事的有两个较年轻的学生，亨德里克·齐加尔斯基和耶日·鲁日茨基。现在，雷耶弗斯基也开始潜心研究密码。

寻找对密码学感兴趣的青年数学家

这三位数学家很快得到华沙密码机构提供的职位。波兰语中密码机构被称作“byro szyfrov”。三人被安排在 BS4 部门。这是一个专管德国密码和电报的部门。华沙密码机构已获得一项重大成功。1920 年，波兰军方在毕苏斯基元帅指挥下在华沙城门口挡住布尔什维克的进攻，密码机构功不可没，因为它破译了俄国人的密码。直至 1928 年，德国防军的密钥已不再给 BS4 造成任何困难。尔后德国人启用一套新的密码系统，投入使用“恩尼格玛”机。波兰人准确地猜到，在新密码后是一种类似于舍尔比乌斯式密码机的机器。

攻克“恩尼格玛”机的战争在和平中开始。不知何时，波兰密码机构通过一个瑞典联系人弄到一台民用“恩尼格玛”机。这台早就能在商店中买到的机器是波兰人所熟悉的，但是德国国防军和以后的纳粹国防军使用的“恩尼格玛”机的密钥轮已改变了接线方式。BS4 部门正确估计到目前启用的机器装有互动轮。因此它也有与生俱来的弱点。

尔后，一次偶然的事件帮助了波兰密码机构。[1] 1928 年的一个星期五，一位驻华沙的德国使馆官员出现在海关并焦

---

[1] 布赖恩·约翰逊：《绝密：第二次世界大战中的科学和技术》，斯图加特，1978 年，第 328 页。

急地询问一只从柏林外交部发给德国使馆的箱子。他坚持要求海关立即放行。他的激动神情令波兰海关人员心里犯疑。他们猜测，由于疏忽，这件外交行李被当作一般货物送往邮局。海关不得打开外交行李，但能检验一般货物。他们耸耸肩声称还未收到。当这位德国人离去后，海关人员将此事上报波兰军事保安机关。箱子被拆开，展现在他们眼前的是一台用稻草精心包装的全新"恩尼格玛"机。周末，BS4 机构仔细检查了这台机器。周一，德国使馆领回这只箱子。它未留下一丝被私自拆封的痕迹。虽然波兰人由此了解了许多有关"恩尼格玛"机的情况，但远未知晓一切，因为研究其内部结构是一回事，用它把加密的消息还原为原文是另一回事。

"恩尼格玛"机密文的开头 6 字母

当来自波森的 3 位年轻的波兰数学家会聚华沙时，就是这种情况。第一年他们就取得一项重大成就。如前所述，用"恩尼格玛"机加密的消息在明文的开头含有两次密钥的三码组，如当日密钥所要求的那样，用于基本位置的机器加密。

我们再来回顾"恩尼格玛"机的工作方式。对轮子的每次调节就是给每一个键，即每个明文字母配一个指示灯，即一个密文字母。每次重新调节则产生一次新的字母表的排列。明文是否真能被如此妥善隐藏起来，就像人们采用无限长的随机数字绦虫（参见第七章）那样？这种呆板的模式有 3 个弱点：

1．给最初 6 字母的加密始终围绕着当日密钥在变化，即一整天使用机器的同样的起始位置。

2．每份截获的消息的第一个六码组有两个相同的三码

组作为明文。如果电文以六码组 DMQVBN 开头，第一个和第四个字母对应同一个明文字母，它们只是采取不同的排列加密。这样一来，第二个和第五个，第三个和第六个也相同。

3．互动轮大大削减了可能的排列数目，由此所有的排列都是对合的。

因此机器远比德军指挥机构所想象的容易测度。"恩尼格玛"机的弱点最终使波兰人能够阅读德国人的无线电报。如果 BS4 机构人员每天截获大量密文，这就会给他们提供众多有关"恩尼格玛"机为当日密钥所规定的最初 6 个排列的情况。在和平的演习中，波兰人每天已掌握近百条消息，它们都以"恩尼格玛"机的同一种起始位置加密。这已足够让人搞清密文的密钥、当日密钥以及渐渐弄清楚密钥轮内接线和插板的接线方式。

事实上 BS4 人员的破译工作变得更加容易。加密员出于方便，常常选用 3 个相同字母，或"恩尼格玛"机键盘上相邻或成对角线的 3 个字母作为密钥。慕尼黑数学家弗里德里希·L·鲍尔[①] 列出 65 份第二次世界大战中某天曾采用的密文六码组。其中仅 SYXSCW 组合就出现 6 次。显而易见，译电员经过深思熟虑选用 AAA 作为报文密钥，这样随着当日密钥每次出现相同的六码组。RJLPWX 组合出现 4 次。同样它还以奇特的密钥 BBB 作为基础。这种轻率使得 3 位波兰数学家在有些日子里不缺少使用相同密钥加密的无线电报。

这种操作程序造成的另一弱点就是加密一条至关重要的开头为六字母的消息时，大多只转动第一个密钥轮，而其他的则处于静止状态。1932 年 12 月，华沙工作组得到的资料使他

① 《破译的秘密：密码学的方法和原则》，柏林/海德堡，1955 年，第 327 页。

们的工作变得更加容易。

德国间谍和被谋杀的参谋长

1931 年初，德国国防部的一个年轻工作人员，汉斯·蒂洛·施密特和法国保安处取得联系并向其提供密码情报，其中也有关于“恩尼格玛”机的信息，当然都是付报酬的。他的代号是 HE。按照法语，这两个字母的发音听起来像德语词“灰烬”(Ache)。起初，法国人并不信任间谍“灰烬”。德国人想把他作为双重间谍安插在法国保安处吗？但密码机构负责人，上尉古斯塔夫·贝特朗，下面还会谈到他审讯施密特后得出结论，“灰烬”确实能提供有价值的资料。在欧洲各个城市的多次接头中，“灰烬”转交的东西中有一份德国陆军服役条例中有关“恩尼格玛”机操作规程的复印件以及 1932 年 9 月和 10 月间使用的当日密钥，即每天密钥轮的起始位置，圆环位置和插板的连接。此外在与贝特朗会面时，常有一位代号为“君王”的法国间谍在场。他必须充当翻译，因为“灰烬”不会说法语。[①] 早在 1932 年 12 月，贝特朗就已把资料寄往华沙。那儿的人员搜集了上一个月的足够的无线电报，此时，他们不仅能够事后破译，而且同时从对密文和明文的比较中进一步了解“恩尼格玛”机密钥轮内部的接线。1934 年，波兰人掌握了“恩尼格玛”机密码。此时他们已能阅读德国纳粹国防军和保安机构之间往来的无线电报。

1934 年 6 月 30 日截获的一份电报，提供下列明文：“告所

① 德军占领法国之后，“君王”出卖了间谍“灰烬”。1943 年 7 月，“灰烬”被处以极刑。

有的机场交出恩斯特·勒姆，不论死活”。这就是“长刀之夜”的指令。这一天，希特勒和他的部长戈培尔在慕尼黑指挥对冲锋队的老战友们展开一场血腥的屠杀。最有名望的牺牲者为参谋长罗姆，他是希特勒攫取政权时期希特勒的一个朋友。不仅罗姆和他的随从遭到暗杀，希特勒借此机会还铲除异己。但我们还是回到华沙破译人员身边。

用“炸弹”机对付“恩尼格玛”机

正如我们所知，当时德国人一直担心“恩尼格玛”机的秘密被泄露，因此他们当然想避免密码被发现。波兰人试图与他们齐头并进。甚至知道接线还需很长一段路要走，从前 6 个字母出发，推断圆环位置，机器的基本位置和插板的连接，对此需要众多用同一当日密钥加密的消息。

伴随着“恩尼格玛”机的每一个新的日期调整，波兰密码学家必须从头开始。即使是纯机械式的工作，这也很费力，可以让一台机器完成这项任务。为此，三位科学家研制了一台图 10.1 中勾划出的机器。它有两套各含 3 个密钥轮的装置，其接线方式和“恩尼格玛”机一样。各自均能调节。另外每套装置都配有 26 个指示灯和同样多的开关。这台机器并非用于加密，也非用于脱密。它的唯一任务是认出轮子处于不同位置时产生的字母频率转换的特征。为此，波兰人演示了所有可能的位置，以便从闪亮的灯的数量上发现随之产生的密码特征。他们演示了 26 × 26 × 26 = 17576 种轮子所处的位置，也找到一些产生的排列规律。这台机器被称作“循环测定器”。BS4 人员利用它制造了一个目录，这使他们有可能在几分钟内根据截获的少数无线电讯找出当日密钥。这是 1938

年秋天的事。在此期间,希特勒已占领奥地利并向捷克斯洛伐克德语区挺进。

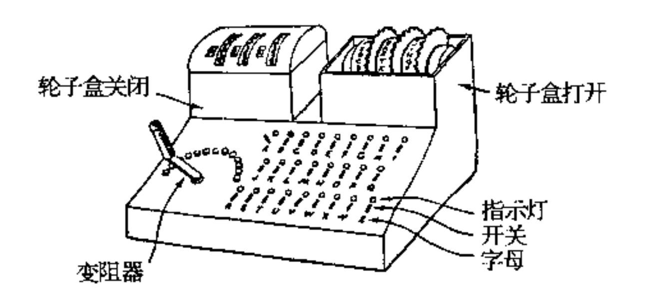


图 10.1:波兰密码学家的"循环测定器"含有密钥轮,它模拟"恩尼格玛"机内的密钥轮。利用这台机器能够研究运用"恩尼格玛"机获得的密码特征并对其进行编目。

华沙的 BS4 部门不能满足于"循环测定器"所取得的成就。1937 年 11 月 1 日,德国人采用新的互动轮,并于 1938 年 12 月 15 日把可供使用的密钥轮从 3 个增加到 5 个。每次把其中的 3 个装入机器。在机器内,这 3 个轮子有 6 种排列方式。从五轮中选出 3 个按不同顺序插入,总共有 60 种可能性。现在,波兰破译者必须演示的可能性数目达 10 倍之多。"循环测定器"力不从心。波兰人制造了一台名叫"炸弹"的更为复杂的机器,值得注意的是这并非空投炸弹,而是冰冻布丁圆蛋糕之意——不管怎样在一年前的西班牙内战中,格尔尼卡城被意大利和德国空军炸毁。他们利用这样一台"炸弹"机模拟 6 台"恩尼格玛"机。研制的 6 台"炸弹"机无一幸存于世;今日已无人确凿知道这种机器的运行方式。

在欧洲,波兰的局势日益危急。1939 年 3 月,希特勒占领了波希米亚和摩拉维亚的余下地区。他的下一个侵略目标是波兰不言自明。希特勒最终肆无忌惮地表示,要夺回依照

《凡尔赛和约》失去的土地。这儿所指的是波兹南和克拉科夫这些波兰城市和从德意志帝国版图中割让出去的东普鲁士地区——波兰的走廊地带。因此迫切要求遭受威胁的国家的秘密警察联合起来。

1939年7月25日,波兰、英国和法国秘密警察代表在华沙附近的皮吕会晤。与德国间谍"灰烬"合作的贝特朗上尉属于法国代表团。波兰人把有关"恩尼格玛"机的研究成果转交给同盟国。此时用五密钥轮加密的密码仍未被破译。人们决定分担这项任务。波兰人将继续从事数学理论工作。法国人试图通过联系人从德国刺探到有关扩充密钥轮组的情报。为破译五密钥轮密码,英国人最后接受研制大量"炸弹"机的任务。另外,波兰人送给法国人两部自己仿制的"恩尼格玛"机。

不久,希特勒对波兰宣战。第二次世界大战爆发。

逃亡中的三位数学家

希特勒的部队越过波兰边境一周后,华沙的密码机构被解散。全体人员乘坐一辆专列前往布列斯特-利托夫斯克,从那儿乘汽车去波兰和罗马尼亚边境。当破译者被来自西方的德国国防军逼得逃亡之时,红军越过波兰东部边境。希特勒和斯大林达成协议瓜分波兰。许多人包括波兰政府在内离开沦陷的波兰,取道前往罗马尼亚。途中火车遭到飞机不断扫射。BS4机构人员认为必须销毁随身携带的"炸弹"机。这三位数学家只有雷耶弗斯基重返故乡。

难民在任何地方都不受欢迎。罗马尼亚人把入境的波兰人关进拘留营。但是三位数学家成功地登上一辆正巧去首都的列车,他们期望驻布加勒斯特的英国使馆能帮助自己去英

国;参与华沙会晤的英国人当时表现出合作的态度。当三人向使馆求助时,他们被"过几天再来吧"这句话给打发了。由于违反了罗马尼亚拘留营的规定,他们害怕随时会遭到罗马尼亚警察的逮捕。此时,处于困境中的他们探访了法国使馆。在那儿,他们受到热情接待,并且立即拿到去法国的签证。赢得波兰数学家与法国密码机构合作,法国人对此饶有兴趣。古斯塔夫·贝特朗特地前往罗马尼亚寻找他的波兰同事。贝特朗还找到许多从华沙逃亡出来的科技人员。他们参与仿制"恩尼格玛"机的工作并研制了"循环测定器"和不少个"炸弹"机。

贝特朗把他们全部安顿在维尼奥勒城堡内,巴黎东南面的格雷阿尔芒维勒尔的一座宫殿内。城堡的代号是"布鲁诺"。这个破译班子立即展开"恩尼格玛"机的仿制工作。对此,在远离巴黎零星分布的工厂里定购零件——谁也不能猜出单个部件的实际用途——,随后在"布鲁诺"组装。此时仍未破译五密钥密码。"布鲁诺"还和英国秘密警察合作,后者已开始自行研制"炸弹"(bomas)机,此时在英语中被叫做"bombes"。

"布鲁诺"的波兰组和英国保持密切联系。1940 年 1 月中旬,28 岁的剑桥数学家爱伦·图灵拜访了他们,他后来在英国成功地领导了针对"恩尼格玛"机的战斗。"布鲁诺"和英国同行通过电传打字机交换消息,那绵延 600 公里的电缆穿过英法区域。这样电话线势必有被搭线窃听之虞。为防止德国人也读出电传打字电报,密码学家们使用自己仿制的"恩尼格玛"机加密电传打字。他们自己也明白破译此密码的难度。偶尔他们也模仿德国人的"恩尼格玛"机消息的风格,并以"希特勒万岁!"结尾。自 1940 年 6 月起,"布鲁诺"能把脱密后的

“恩尼格玛”机电文发往英国。

在此期间，德军向法国、荷兰和比利时推进。距离格雷斯－阿曼维利耶只有几公里之遥。“布鲁诺”办公室必须尽快转移。他们在巴黎稍作停留，在那儿他们24小时不间断地破译不断推进的德军的无线电报。尔后，他们必须转移。在向南方逃亡过程中，他们仍在处理截获的无线电报。当法国投降时，贝特朗随同15位波兰人和7位西班牙人一起飞往阿尔及利亚。西班牙的破译人员在研究意大利军队之间往来的无线电报。10月1日，工作组在于泽斯，尼姆东北部的富泽城堡中设立了一个新的办公室。掩饰名为“卡迪克斯”。这个集体自己的代号是“300组”。此时的破译人员处在亲德的维希政府统治区。目前工作组的任务就是把破译的无线电报发给英国人。“300组”破译了600多条发给陆军元帅隆美尔统率的北非德军的消息。

1941年底，三位波兰数学家中最年轻的鲁日茨基在法国密码机构驻阿尔及利亚的分部工作了相当长的时间。他搭乘法国客轮《拉摩谢尔》号重返维希统治下的法国，情况至今不明，这艘船是触礁还是撞上了水雷；鲁日茨基被列入死亡者的名单。

1942年9月，贝特朗获悉一支德国特别小分队到达蒙彼利埃来测定秘密无线电台的位置。为了将破译的发给德国非洲军团的无线电报发往英国，“卡迪克斯”使用从英国偷带来的电台。德国人找到这部电台只是时间问题。实际上德国人已不规则地在白天与黑夜切断地区间不同区域的电流，以便从发报机的中断上辨别它所处的区域。11月6日，德军的无线电探向器搜索邻近的两家农民住宅。因此，“卡迪克斯”迅速转移。几天后，希特勒的部队向在此之前尚未被占领的维

希法国进军。城堡也落入德军手中。

雷耶弗斯基和齐加尔斯基试图前往英国。他们必须绕道经西班牙、葡萄牙和直布罗陀海峡，并一再被逮捕。8个多月后，他们到达目的地，加入流亡在英国的波兰军队并受命破译党卫军的规则游戏密码。

我们不完全明白为何不让这两位天才的密码专家攻克那些的确棘手的难题。英国人不知怎么地不愿相信，波兰人在对“恩尼格玛”机的脱密方面已有相当大的进展。从此，英国新设立的新项目“超级”任务就是处理用“恩尼格玛”机加密的无线电报，而波兰人再也没有被吸收加入这项工作。自1939年8月起，在伦敦北部的古特·布雷契莱庄园里成立了几千人参加的，从事破译“恩尼格玛”机无线电报的庞大机构。第二次世界大战结束30年后，雷耶弗斯基对此才略有知晓。

第二次世界大战接近尾声时，在西方大约有2万名波兰士兵。其中只有10%的人愿意返回共产主义的波兰，雷耶弗斯基也是其中一员。回到波兰，他在一家高级中学谋求数学老师的职位，但毫无结果。他怎样度过随后的岁月，世人知之甚少。1980年，当时的波兰政府发布的官方悼词令人困惑地说他在皮得哥什(布罗姆堡)管理机构的不同部门工作了20年，并于1967年退休。

雷耶弗斯基最后的破译

1976年夏天，雷耶弗斯基应一位在第二次世界大战中结识的、现住在英国的波兰人的请求，破译一份于1904年加密的信件。当时的波兰一部分属于俄国，一部分属于德国，而波兰社会党领导人约瑟夫·毕苏斯基寻求国际援助以建立一个

独立自主的波兰。他也向当时和俄国打过仗的日本求助。在这个时期产生大量无人能够破译的加密文件。马利安·雷耶弗斯基的本领又一次受人关注。但他拒绝了。此时摆在他面前的复印件一塌糊涂,边沿缺字,其余的地方无法辨认。如果人们读到他在华沙的一位朋友的信件,知道雷耶弗斯基几乎是被迫地破译了这封加密信,就会联想起柯南道尔对歇洛克·福尔摩斯工作情形的描述。

雷耶弗斯基本来想和家人一起外出度假。然而后来,雷耶弗斯基夫人告诉那位朋友,自己丈夫的举止行为奇怪。他独自咕噜着在房内踱来踱去达数小时之久。他突然想让家人去度假而把自己一人留在华沙。过了一段时间,这位朋友接到雷耶弗斯基的电话要他过去一趟。当他到达雷耶弗斯基那儿,他看见了精疲力竭,完全变样的雷耶弗斯基。他骞地把一张纸递到他眼前,那是他上几个月的劳动成果。

雷耶弗斯基破译了1904年的密文。当他把明文寄给伦敦的委托人时,同时告诉他自己不希望再收到这样的文章。[①]

大凡战争结束,授勋仪式会接连不断,但是秘密警察的功臣们却默默无闻。战争结束时,雷耶弗斯基和齐加尔斯基被提拔为少尉。齐加尔斯基留在英国,在一所学院执教并于1978年去世。同年,人们要授予住在波兰的雷耶弗斯基名誉博士的称号,但他对此不感兴趣。战争结束大约30年后,贝特朗向世人披露他在法国作出的贡献。现在,人们把他的生平搬上电影和电视。雷耶弗斯基于1980年去世,享年74岁。这位德军"恩尼格玛"机的征服者是为盟军战胜纳粹德国作出

---

① 瓦迪斯瓦夫·科扎克茹克,"向旧式'恩尼格码'机发出的新挑战",《密码学》,1990年7月,第204页。

实质性贡献的人员中的一个。

1964 年,世界新闻界报道了三位波兰密码学家中的一位名字:在东京举行的奥运会中,一位美术学院大学生为波兰队争得一枚银牌。他是 1941 年在一次海难中丧生的耶日·鲁日茨基的儿子。

布雷契莱庄园的人们

1939 年 7 月,参加华沙会晤的英国代表团成员之一的海军中校阿利斯泰尔·丹尼斯顿,是国家代码与密码学校的负责人。早在第一次世界大战期间,作为密码学家的他就在海军部中著名的“40 号房间”就职。被描述为冷静,有些审慎的他当时大约 50 岁。

深谙密码部门重要性的英国征用了一所庄园。它位于布雷契莱附近人迹罕至的地区,在伦敦北部约 70 公里处。1939 年 8 月,丹尼斯顿密码学校迁移至此。密码学家在以前的马厩里开始工作。除了丹尼斯顿,加入他们队伍的还有其他“40 号房间”的元老,如威廉·F·克拉克以及奈杰尔·德·格雷,他是最早掌握齐默尔曼——电报密文的人中的一个。现在有必要继续征募专业人员。剑桥大学的数学家是首要人选。

那儿年轻的英国数学家爱伦·马蒂松·图灵刚从美国回来。1912 年生于伦敦的图灵,19 岁中学毕业后进入剑桥皇家学院求学。4 年后,他因出色的博士论文赢得一笔奖金。1936 年至 1938 年间,他在美国新泽西州的普林斯顿大学就读。他在那儿研究数理逻辑与电子计算机理论。虽然当时的电子计算机尚未问世,但是对它的工作方式已展开了先行性理论研究。战后在研制第一代计算机过程中,图灵起着举足

轻重的作用。他在布雷契莱庄园内第一次认识"恩尼格玛"机并了解了波兰"炸弹"机的细节。

在此再一次回顾当时的局势:波兰人能阅读有五轮置换的三密钥轮"恩尼格玛"机无线电报,德国人又启用了两个,尔后又增至8个密钥轮,这使得破译密码更为复杂和费时。德国人还改变电文密钥传送方式。1940年5月,电文的开始不再出现对破译大有裨益的6个字母。演示所有可能的调节机器的方法变得更加麻烦。

此时的图灵正研制英国"炸弹"机,它比波兰人的"炸弹"机更有成效。"炸弹"的极为精细的部件需要保养及维修人员。需要报务员整天在有关频率中等待信号并截收无数的无线电讯。尔后,起着关键作用的破译者才能着手工作。把辅助人员计算在内,大约有一万人在布雷契莱庄园工作。

英国"炸弹"机在每天截获的几千份无线电讯中搜寻军事用语中常用的如"oberkommando"(上级命令),"fuehrerhauptquartier"(元首大本营)或者"kommandeur"(指挥官)之类的术语。186页中就已阐述的"恩尼格玛"机的特性帮助了破译者,即无论怎样调节,明文字母和密文字母不可能一致:这就是互动轮的灾难。例如密文某处出现字母F,他们就确信这不可能是"fuehrerhauptquartier"的起始处。人们只需把明文"fuehrerhauptquartier"写在条带上并放至密文下,一旦明文密文的同一处出现同一字母,那么这就不可能是明文所处位置。

让我们观察一下图10.2上部所示的由87个字母组成的一条简单密文。如果它是按明文密文字母相异的原理加密,而且明文中出现"fuehrerhauptquartier"一词,那么文中只有28个字母是这个词可以着手的地方。例如情况是明文字母恰好

一开始就处在密文下面(图 10.2 中),这样,上下对应的明文密文字母各不相同。如果向右移一格写下明文:T 与 t 上下重叠,情况就不再一样。图 10.2 下部,在密文下方用点表示 28 种明文词可能开始的地方。原则上就各种可能性而言,人们可以演示密钥轮的所有位置,以便弄清,其中是否有一个位置能把明文词转入相应的密文词组。如果"fuehrerhauptquartier"这个词在文中根本未出现,那么这种方法当然也失灵。[①]

fuehrerhauptquartier

图 10.2,上:一段通过置换得到的密文如同在"恩尼格玛"机密码中,没有明文字母被转换成同样的密文字母。估计这段密文的明文含有"fuehrerhauptquartier"一词。

中:密文中明文词"fuehrerhauptquartier"可能出现的位置。在这个位置中上下没有相同字母。

下:密文字母下方用点表示经过猜测的明文"fuehrerhauptquartier"可能的位置。

---

① 我在此列举了一条密文,它的明文含有"fuehrerhauptquartier"。不过,这不是根据"恩尼格玛"机原则加密的,而是选择了简单的单码密码。它与"恩尼格玛"机特征一样,不会将任何字母转化成其身。读者看到此处可以毫不费力读出明文。

英国人有时甚至试图在德国人的无线电报中插入某些特定词。例如:如果他们派飞机炸毁标志重要航道的光标,他们就可等待德国船只通过无线电报被告之此航标的消失。这样在报文中就极有可能出现加密词"Leuchtboje"(光标)。因此这座被炸毁的光标指引了通向正确密钥轮位置的路径。

在布雷契莱庄园的"行话"里,人们称一份无线电报中可能的明文词为"cribs"。为了以可能性最大的密钥轮位置,圆环顺序,密钥轮顺序,插塞连结对明文进行加密并查明由此产生的字母组合是否在截获的无线电报中出现,"炸弹"需要"cribs"。如果在调节"炸弹"时情况是这样,那么它极有可能是按照为加密无线电报所用的当日密钥调节的。就是呆板的称呼如军衔和职位等也提供大有帮助的"cribs",因为它们在明文中经常出现。布雷契莱庄园有一份目录,上面罗列了按照各种可能的当日密钥加密"eins"的密码。由于"恩尼格玛"机无法加密数字符号。德国人必须把数字以字母形式变成文字。因此研究"恩尼格玛"机无线电报,弄清明文是否含有"eins",也很有价值。

布雷契莱庄园的破译者不必总是让"炸弹"机演示密钥轮所有可能的调节方式。第二次世界大战期间,德国人禁止一个月内两次采用同样的密钥轮位置。"炸弹"机在一个月时间不断流逝的情况下,需要演示愈来愈少的位置;而不是密钥轮所具有的60种可能性。

对英国破译者而言,另一帮助就是既用"恩尼格玛"机,又用一种较容易解密的体系来给无线电报加密。例如布雷封锁航道,不仅必须采用"恩尼格玛"机体系既向德军潜艇,而且也向扫雷艇发出警告,而扫雷艇使用一种较简单的、盟军已掌握的密码体系。

英国"炸弹"机是货真价实的巨型计算机。它约含有33个密钥轮的机器。密钥轮是由电力驱动的。"炸弹"机发现密文中一个所需要的词可能要花数小时时间。有时只需10分钟就能找到密钥轮正确的顺序。图灵设计的第一台"炸弹"机于1940年投入使用。尔后,数学家戈登·韦尔什曼成功地对机器进行改进。1941年末,布雷契莱庄园内有12台这样的机器以供使用。1943年3月,增至60台。就是这样,有时为了查出一个当日密钥,计算机需要连续工作3天。1940年春天,德军远征挪威期间,布雷契莱庄园已成功破译第一批密码。一年之后,英国人已能阅读"恩尼格玛"机发出的主要的无线电报。在挪威外被击毁的一架德国飞机内发现一台"恩尼格玛"机,机器以及密钥本被交到他们手中。远征法国途中,德国的一支情报部队和他们的坦克冒险推进,深入腹地被俘获。盟军从俘虏那儿找到更多的资料。1941年5月,英国海军缴获一艘德国潜艇,同样带有"恩尼格玛"机和密钥本。这一切获得的信息推动了"炸弹"机的进一步发展。

爱伦·图灵的悲剧命运

1939年9月4日,即希特勒突袭波兰3天后,27岁的爱伦·图灵到布雷契莱庄园工作。早在普林斯顿逗留期间,他就从事密码学的研究。他考虑怎样用数字代替字母,然后把它们和一个秘密数字相乘,把得到的结果作为密文发出。1937年,当他首次意识到英国可能会被卷入对德战争时,他认为这数字位数必须足够长,足以使百来个德国人每天工作8小时,花费几百年的时间通过系统实验才能发现秘密因子。图灵还思索了怎样用电路接通做乘法,而且他自己研制了一台这样

简单的电动式计算机。

图灵在布雷契莱庄园工作可谓人尽其才。早在1940年1月，他就前往法国拜访了在"布鲁诺"工作的波兰数学家，他们的"炸弹"机深深地吸引着他。从波兰人那儿得知的信息加上自己当初的考虑也许就诞生了图灵式"炸弹"机的设想。英国史料只是轻描淡写地记下两方数学家会面的情况。这是英国人不想突出波兰数学家的贡献的又一表现。

战后，图灵在国家物理研究室从事制造一种大型计算机。自1948年开始，他领导曼彻斯特大学的计算机研制工作。他一直思索：一台机器能思考到什么程度，用它做的事又能达到什么程度，我们今天把这称为"人工智能"。

天才的数学家爱伦·图灵是个同性恋者。由于天性使然，他觉得这是理所当然，不必遮遮掩掩，他没有任何负罪感。他希望同性恋很快在大不列颠合法化。然而"根据1885年刑法修订本第十一条，(这是)伤风败俗的行为"。[①] 他的同性恋最终给他带来灾难。1951年12月，他在大街上遇见一位19岁的失业者，阿诺德·默里。这两个不相配的同伴之间迅速发展到一种性关系。不久，图灵有理由怀疑默里，因为他一再向自己借钱并且从不归还。他也许还偷过图灵一次。

1月23日，图灵的住所被盗。不过只丢失了不多的物品，总价值约为50英镑。当图灵质问同伴时，他向图灵保证自己没有参与盗窃，但是他曾向一位同是失业者的熟人谈起图灵和他的住所，随后这人唆使他入室偷窃。他拒绝了，但他确信破门盗窃是那位熟人干的。

爱伦·图灵报警失窃。他的陈词自相矛盾，以致警察不费

---

① 安德鲁·霍奇斯：《爱伦·图灵，"恩尼格玛"机》，柏林，1989年，第528页。

吹灰之力就查清楚他与同伴，还有那位无名的第三者之间关系的真相。因此数学家爱伦·图灵成为法律面前的罪人。1952年3月31日，“女王反对默里和图灵”的诉讼得到受理。两人都在被控的所有方面(与男性有恶劣的伤风行为)承认有罪。默里的辩护律师成功地把主要责任推卸到年龄较长的图灵身上，说是他引诱了自己的当事人参与犯罪。图灵被判为一年徒刑，但得到缓刑，条件是接受一种化学治疗。他选择“器官疗法”取代入狱，这种疗法使他在治疗期间变得性无能。图灵保住了大学里的职位。1952年5月，人们甚至决定给他在曼彻斯特大学提供一个计算机理论的特别讲席。尽管在此期间，英国舆论对同性恋的态度宽容了一些，图灵还是承受着治疗的耻辱并丢尽颜面。

6月8日，图灵的女管家发现他口吐白沫死在床上。死因是氰化物中毒。警察在屋内发现一瓶氰化钾与一瓶氰化物溶液。床边还有一只啃过的苹果。调查人员忘记对苹果进行化学分析。图灵也许把它浸在氰化物中。法院调查得出结论是自杀。罗尔夫·霍赫胡特在小说《爱伦·图灵》[①] 中写道，1963年以前出版的《不列颠百科全书》中只字不提这位数学家，尔后出版的书中将其称为逻辑学家和现代计算机的一位前驱——“图灵”式机器的创造者。霍赫胡特就图灵在战争中对英国所作的贡献时指出：“他的卓越成就使他成为除了丘吉尔之外，也许无人能与之匹敌的救星，但人们对他的贡献只字不提……他们也相应写道，虽然他服毒自杀，但也许不是故意自杀，而是实验性的。他们没有提及他的同性恋诉讼案……但只字不提图灵破译‘恩尼格玛’机，真是无耻之极。”

---

① 赖恩贝克，1987年，第165页。

重归第二次世界大战期间图灵的"炸弹"机破译德国"恩尼格玛"机电文的布雷契莱庄园。在那里工作的每个成员必须保证对参与的活动保持终身的缄默。因此战后前 30 年内，公众对以图灵为核心的密码学家们的功绩一无所知。尔后，古斯塔夫·贝特朗的战争回忆录在法国出版。攻克"恩尼格玛"机的战斗已不再是秘密。1974 年，弗雷德里克·W·温特博特姆在英国出版了书名为《超级秘密》[①] 的回忆录。"超级"是布雷契莱庄园内对破译"恩尼格玛"机消息的代称。

向希特勒坦露计划的间谍

无线电报立即被转至负责部门，也直接送到温斯顿·丘吉尔首相手中。温特博特姆就是布雷契莱庄园和政府部门间的一位联络人。

1917 年 7 月 13 日，第一次世界大战期间，德国的一架战斗机在比利时上空击中一架远在德国战线后面的英国的尼厄波尔式飞机。坠机着陆后，一位德国军官从飞机残骸中拉出受伤的飞行员，温特博特姆。这位英国人做了 18 个月的德军俘虏。在此期间，他不仅治愈了骨折的鼻子，而且还有时间和闲情学习德语的基本知识。当时他对德国人的了解就决定他未来的一生。他根据战败德军军官的谈吐认为，德国迟早会对在第一次世界大战中遭受的失败报复，他对此坚信不移。

他回到英国后学习法律，试着做农场主，1930 年以后为英国秘密警察空军部队效力。当时还禁止德国人拥有自己的空军。但有消息传到伦敦，俄国人训练德国飞行员。对此进

① 伦敦，1974 年。

行调查正属于温特博特姆的工作范围。1930年前后,希特勒领导的德国国家社会主义工人党(NSDAP)羽翼丰满。温特博特姆动身前往德国,由伦敦《时报》记者介绍,他与阿尔弗雷德·罗森堡建立联系。罗森堡是德国国家社会主义工人党的主要理论家,1933年,希特勒攫取政权后,他成为外交政策部门的领导人。第二次世界大战中,他出任德国东部占领区的帝国部长。1946年在纽伦堡对主要战争罪犯审讯中被判死刑并被处决。英国间谍温特博特姆和德国部长保持了将近8年的联系。

早在1933年以前,罗森堡就邀请温特博特姆访问德国,并向他介绍当时许多有影响的人物,其中也包括希特勒。当时的国家社会主义者认为值得与英国保持良好关系。当时大权在握的希特勒在1934年与这个英国人的一次谈话中明确指出:"世界上只应存在3个强国,英帝国,美利坚合众国和德意志帝国。"他继续说道:"我们只不过希望英国满足于自己的世界帝国,而且不妨碍德国的扩张计划"。[1] 另外,温特博特姆也安排罗森堡访问英国一次。

这几年中,温特博特姆不仅是希特勒领导集团的座上宾,而且在将军们那儿也炙手可热。他把在这期间获得的情报同其他间谍送往伦敦的情报综合一处。弗雷德里克·温特博特姆不是詹姆士·邦德,他从不暗地里给文件拍照,不把文件加密送往伦敦,也不试图偷偷地溜进一些地方。他是受邀请而来,在任何地方都不必窃听,他的对话伙伴闲谈时,他只需倾听。

① 弗雷德里克·温特博特姆:《纳粹关系》,伦敦,1978年,第70页及以下几页。

温特博特姆对德国人迅速扩充空军尤其大吃一惊，对此他懂得一些。他在回忆录中一再抱怨伦敦对他发出的警告常常置若罔闻。[①]

他和帝国当权者于1938年秋断绝关系。他的对话伙伴越来越审慎，因为靠他对英国政治家施加影响似乎是不可能的，他们失望了。当纽伦堡的党代表大会结束后，温特博特姆向罗森堡辞行时，双方也许都明白彼此将不再有重逢的机会。

回到英国后，温特博特姆转向另一种侦察——空中照相侦察。这在当时只是处于萌芽阶段。温特博特姆成功地在美国公司生产的一架"洛克希德"飞机内安装了一台隐蔽式照相机。在所谓的民用飞机飞行时借用它可以拍摄到德国新建机场的情景。

正如温特博特姆报道的那样，"洛克希德"飞机在莱茵河畔的法兰克福飞行博览会上展出，机内妥善地隐藏了秘密照相机。当时的空军总参谋长艾伯特·凯塞林恰好对这架飞机产生浓厚的兴趣，并询问飞行员是否允许他试飞一次，这位平时执行间谍飞行的驾驶员答应了他的请求。当飞机掠过莱茵河上空时，凯塞林异常兴奋。这时飞行员发觉下方出现他以前飞行中还未拍过照的建筑。他悄悄地打开照相机。就这样，德国空军总参谋长万万没有料到自己竟参与了英国秘密警察的间谍摄影。

---

① 我不知道温特博特姆以后给其上司的报道可信度有多高。他在回忆中写道，他把派给自己的那名德国陪同人员称为"查理"，因为在德语中有"guten Karl"的习惯用语，在此他也许混淆了karl和kerl。尔后，他有关港口城市wannemüde的报告指的也许是Warnemüde（瓦内尔明德），他写Danziger Goldwasser（但泽利口酒）用的是Danziger Geldwasser，并还提到慕尼黑附近的泰根湖。

在成功道路上的“超级”机

第二次世界大战期间，温特博特姆和其他人一起负责分析由布雷契莱庄园破译的“恩尼格玛”机电报。30 年后，第一批人打破沉默，披露了布雷契莱庄园的工作情形，温特博特姆就是其中一员。

英国人早在大战爆发的第一年就已钻研德国人的通讯往来。因此，布雷契莱庄园破译了赫尔曼·戈林宣布空中打击英国的“鹰计划”。丘吉尔立即收到文本的复印件：

帝国元帅戈林手谕：所有空军部队，23 号，5 次山鹰行动，在最短的时间内从天而降袭击英国空军，希特勒万岁。

采取“山鹰”行动的消息源源不断地到达。“超级”能够密切注视着准备工作。当袭击来临时，英军已严阵以待。德军轰炸机第一次在大海上空就遭到打击，只有少数几架侵入。第二次袭击时，德军损失惨重。

戈林的计划如下：首先轰炸所有的机场，尽可能炸毁战斗机，然后，把英军歼击机卷入与德军歼击机的较量。人们得知这个战斗计划多亏“超级”，英国人将飞机分散在许多飞机场内伪装好，歼击机并未加入战斗。这一对策在空军内部导致意见分歧，因为绝不是所有的军官都明白戈林的意图。“超级”如此秘密，只有少数核心人物才知晓英国人已能破译“恩尼格玛”机的无线电报。

当戈林的计划落空后，他改变策略，集中力量轰炸伦敦。

人们认为这是他战略上最大的失误。9月5日，他下令出动300架轰炸机轰炸伦敦的船坞。歼击机将为轰炸机护航。他的命令在几分钟内就被传到英国首相丘吉尔手中。这次袭击虽然来势凶猛，由于英国人已得到警告并做好应战准备，使战斗机没有遭到打击。1940年9月17日，德军又发动新的一轮袭击。因为借助“超级”，已对他们严阵以待，攻击又被击退。两天后，“超级”获悉纳粹国防军命令运走放在荷兰的为入侵英国准备的战备物资。英国人有了喘气的机会。希特勒征服英国的“海狮”计划破产。

但是惊恐尚未结束。据温特博特姆的报道，“超级”在1940年11月获悉德军即将空袭考文垂市，他写道，丘吉尔从这一刻起开始面临着一次艰难抉择。如果疏散城市居民，德国人会发现“恩尼格玛”机电报已被英国人获悉，盟军就会由此丧失战争中的巨大优势。丘吉尔面临的难题是，在随后的几天，是使考文垂市民免遭大难，还是着眼于将来拯救更多人的生命而不泄露“超级”的秘密。他选择了后者。为了尽可能减少考文垂市的损失，他命令加强这个城市的消防和救护车力量并严阵以待。这段历史不是没有争议。[①] 温特博特姆1974年出版的书引起人们的普遍反感，因为他在书中只字不

---

① 美国历史学家福雷斯特·伯格和其他历史学家认为，温斯顿·丘吉尔容忍了对考文垂市的轰炸的说法是无稽之谈。（例如见戴维·卡恩：《卡恩的密码研究》，纽约，1983年，第96页）不管考文垂战略的历史背景是什么，如果盟军不想泄露已了解的德国无线电报，就不能充分利用“超级”提供的情报。

当时在“六号棚屋”负责翻译“恩尼格玛”机电报初稿的斯图尔特·米尔纳－巴里对温特博特姆的说法提出异议。他回忆道，虽然当时已了解“恩尼格玛”机的电报中有计划偷袭，但是目的地不是用名称而是用数字标出的。破译者无法预测是哪座城市将遭袭。米尔纳－巴里认为根据回忆，人们等待伦敦被袭击（F·哈里·欣斯利，艾伦·斯特里普，《破译者》，牛津，1993年，第95页）。

提雷耶弗斯基和图灵,并给人造成这样的印象:希特勒放弃入侵英国的计划应全归于"超级"。历史学家认为这夸大了"超级"的作用。[1]

相反,"超级"在大西洋战役进程中所起的决定性贡献是无可争议的。

大西洋战役

1941年9月28日,德军的U67和U111潜艇企图在佛得角群岛用鱼雷袭击"HMS克莱德"船队。一艘英国潜艇突然浮出水面驱逐偷袭的潜艇。德国潜艇部队司令,海军上将邓尼茨,疑窦顿生。在平时人迹罕至的海域,敌军的潜艇及时赶到,这不可能是偶然的。要么进攻遭到泄露,要么德军的无线电报被敌人破译。

4个月后,德军潜艇开始用"恩尼格玛"机加密电报。此时的"恩尼格玛"机已安装了4个轮子,又附加了"希腊密轮",即比其他密钥轮薄一些的β密钥轮。另外,这种新型的"恩尼格玛"机配备了一个薄型的、已改变接线的互动轮。"希腊密轮"与薄型互动轮以及3个老式密钥轮恰好被装入3轮"恩尼格玛"机机罩内。"希腊密轮"与老式的密钥轮有所不同,它在机器驱动时静止不动,始终停留在插入时的位置。如果把它安插在一个在视窗中显示字母A的位置,其电路和薄型互动轮的电路一起产生的效果和老式的厚型互动轮一样。这也意味着在这个位置上,新型4轮"恩尼格玛"机和老式3轮密码机的工作方式相同。这一位置使得交换新旧"恩尼格玛"机加

---

[1] 戴维·卡恩:《卡恩的密码研究》,纽约,1983年,第110页。

密的消息成为可能。这种情况出现在传送如气象预报这类不重要的消息时。

与以往的款式相比，第四个密钥轮使"恩尼格玛"机可能的调节方式增加到原来的26倍。谁想在"炸弹"机上把它们全部演示一遍，工作量陡然增加了26倍。

从1942年1月1日起，德军在向大西洋的潜艇发送电报时启用一种新式机器。此时英国人再也无法弄清德军潜艇逗留的位置，这导致它无法给来自美国的护航舰队指引安全的航线。造成的后果是灾难性的。美国的船坞全力以赴建造船只。然而绝大部分的船只横穿大西洋至多3次后就被击沉。可使用的商船数目不断减少，而德军的潜艇舰队却在增加。

布雷契莱庄园的人们迫切需要更多的快速"炸弹"机，后来命运之神垂青了他们，气象预报成了德军的灾难。

1942年10月底，英国的4艘驱逐舰在海法港附近发现驻扎在墨西拿的德国U559潜艇的踪迹。他们总共发射了288枚深水炸弹，逼迫海德曼指挥官命令潜艇浮出水面。严重遭创的潜艇刚露出表面就遭到四面八方的射击。船员们企图跳水逃生。一些英国水兵向潜艇游去，试图抢出秘密资料。当海水不断涌入内舱时，他们缴获了一本电码本以及当时通用的气象预报的密钥。两名英国水兵再也找不着从逐渐下沉的潜艇中逃生的路径。

这个气象密钥帮助布雷契莱庄园的破译者搞清楚德国海军如何使用四密钥轮"恩尼格玛"机。气象预报是用三密钥轮密码发送的，即"希腊密轮"处于A的位置。布雷契莱庄园的人们不仅能读这些消息，而且借助U559潜艇的气象密钥，他们还知道其他3个密钥轮所处的位置。在加密紧接着的重要无线电报时，德国加密员让3个活动密钥轮维持先前的位置，

只是把"希腊密轮"插至其他位置。但英国人从气象预报中知道了活动密钥轮的位置。因此只需找出"希腊密轮"被插在 26 个位置中的哪一处,一个本质上简单得多的问题。

从 1942 年 12 月 13 日起,德军潜艇的无线电报在布雷契莱庄园内已不再是秘密。有关大西洋上行动的脱密电报每天陆续传来,达到 3000 份。[①] 英国海军在一周后又知道德国潜艇在大西洋停留的地点,护航舰队就能绕道而行。此时建造的船只终于比下沉的多。在大西洋战役中,情况发生变化。

日本人从燃烧的柏林发出的无线电报

1945 年 3 月,从东线推进的苏联部队还能在奥得河—尼斯河沿线和巨人山脉中被暂时阻挡住,但西线已经全面崩溃。盟军渐渐逼近易北河。他们于 3 月 8 日截收一份从柏林发出的电报,电报立即被送往华盛顿附近的美军密码机构。不费吹灰之力就破译出这份电报。这是日本驻德大使大岛浩发出的电报。他从遭受空袭的柏林多次发出加密电报向东京报告情况。大约在 1942 年 10 月 9 日,他报告了访问东普鲁士希特勒大本营的情形。希特勒在密谈中估计来自非洲的盟军将在巴尔干半岛而非意大利登陆。大岛浩早在 1943 年秋天就已参观了希特勒为对付来自西线攻击而修筑的防御体系"西壁防线",并在一份加密的无线电报中详细地向东京报告这一情况。

此时是 1945 年春天,他把消息发给外交大臣重光葵。其中并没有军事秘密,他只描绘了日渐崩溃的柏林状况:汽油

① 安德鲁·霍奇斯:《爱伦·图灵恩尼格玛机》,柏林,1989 年,第 283 页。

异常匮乏，只能在黑市上用咖啡购买到。到处构筑街垒阻碍了城市交通，但主要集中在政府区一带。街垒有2至3米高，厚度有1至2米，都是由囚犯，冲锋队员和妇女们从废墟和瓦砾中堆起来的。①

盟军之所以能破译日本的无线电报是因为它们用被美国人称为“紫色”的机器加密的。这是和“恩尼格玛”机类似的日本密码机，它安有插板，以及如同电话中继站中使用的4个多级开关，还有两台打字机。在其中一台上按键输入明文，在另一台上得到密文。用拉丁字母表达日文词。规定用特定的三码组字母表示标点符号。开始解密时困难重重，只有当错误的信息再次重复时，“紫色”机的秘密逐渐被揭开。威廉·弗里德曼对此作出重要贡献。

“恩尼格玛”机和“紫色”机以及第二次世界大战中美国人使用的“哈格林机器”都是机械式密码技术发展的顶峰。随着波兰和布雷契莱庄园的“炸弹”机问世，开辟了利用电动式机器加密的密码新纪元。计算机被引入密码学中。

---

① 卡尔·博伊德：《围困的苦恼：日本人高水平的无线电情报以及柏林的陷落》，《密码学》，1989年7月，第194页。

22.
33.
144

11

计算机的引入

政府对自己的人民保密,……为什么人民就不许对政府相对保密呢?

——菲利普·齐默尔曼

刑事犯罪分子和恐怖分子滥用密码,这是令人无法接受的风险。

——路易斯·弗里希,美国联邦调查局局长[①]

字母和数字是用于记录和计算的良好的工具。1833年,格丁根数学家卡尔·弗里德里希·高斯和他的同事物理学家威廉·韦伯制造第一台发报机时,他们明白电流只能持续传导电流脉冲。几乎在同时,美国画家及发明家塞缪尔·芬利·莫尔斯也面临同一个问题。他利用长短不同的电流脉冲加密字母和数字。于是莫尔斯电码问世:a是长-短,b是长-短-短-短,……z即长-长-短-短。就连歌德最打动人心的诗歌亦然,

① 这两则均引自《明镜》周刊,1996年,第36期,第200页和210页。

甚至浮士德也能完全被变为一连串长长短短的尖叫声,并当作无线电报送入世界。

人们也可用数字表示莫尔斯电码:长表示1,短即为0,随之得出 a=10,b=1000,……z=1100。与字母表计数(a=1,b=2,……z=26)不同的是,这儿只出现数字0和1。我们还不习惯如此,因为我们使用十进制计算,其中还有数字2至9。我们之所以采用十进制是因为我们有10个手指。只有6个,甚至只有2个手指的人们也采用进位制。这种体系一点也不比我们的逊色。

其他的数字系统

如果在纸上记下一个诸如1997的数字,谁会对此苦思冥想?他当然明白这总共是由1000年加上9个100年,加上9个10年,再加上一个7年得来的。古代罗马人采用另一种形式写出这一数字:MDCCCCLXXXXVII。这对受过教育的罗马人而言也许是一种容易理解的记号表示法——他在读数时就知道它的大小。如果他把两个数字,例如MDCCXLVI和MMCXXVI相加,他就束手无策了。在我们的系统中,我们把这两组数字写作1746和2126。借助我们的数字系统,加法就简单了,结果为3872。

在十进位制中,同样的符号具有不同的意义,如果它们在一个数字的不同位置出现,比如9在1997中。从右边读过来,按次序是个位数和十位数;下一个符号是百位数($100=10\times10=10^2$),然后是千位数($1000=10^3$)等等。做加法时,相同位置的数字相加。如果大于10,我们只需写下超过10的余下部分并向左进一位。按照我们的书写方式,每个数被写成10的幂的和数,仅仅记录下每次10的幂的数:

1 1 1
2 2 2
3 3 3
4 4 4
5 5 5
6 6 6
7 7 7
8 8 8
9 9 9
0 0 0

$$1746 = 1 \times 10^3 + 7 \times 10^2 + 4 \times 10^1 + 6$$

我们称这种数字表达方式为十进位制。因此 10 的作用非同寻常。这是由于人类一开始借助手指计数。在漫长的历史长河中，人类偶尔也加上脚趾，采用二十进位制计算。今天我们在法语中还可以觅到它的痕迹。法语中的 80 并非 8 乘 10，而是 4 乘 20：quatre – vingt。今天的巴黎有所在 13 世纪为治疗 300 个失明老兵而建造的眼科医院，"Hôpital des Quinzes – Vingts"，逐字翻译就是"15 乘 20 的医院"。玛雅人和阿斯特克人也采用二十进位制。图 11.1 所示：在鸭舍内，鸭子唐纳德



图 11.1 鸭舍内所有居民的每只手除大拇指外只有3个手指。鸭子唐纳德和朋友们使用的进位制中，8 和我们进位制中 10 的作用一样(版权© 迪斯尼出版)。

和朋友们的每只手只有 4 个手指(含大拇指),结果只能采用八进位制。计数如下:

1,2,3,4,5,6,7,10,11,……,16,17,20,21……被我们称为 1746 的数字由 8 的幂组成,即:

$$1746 = 3 \times 8^3 + 3 \times 8^2 + 2 \times 8^1 + 2$$

我们写成 1746 的数字在鸭舍中必须叫做 3322。注意:这只是写法不同的同一个数字。

八进位制的加法和十进位制一样,只是 8 代替了 10 进位。我们举出前面已列出的十进位制计算题 1746 + 2126 = 3872。1746、2126 和 3872 转换为八进位制分别为 3322、4116 和 7440。如果十进位制的 3872 是另两个数字相加的和,那么此时在八进位制中也是相应的两数字之和,因为鸭子唐纳德和朋友们计算:

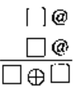
$$\begin{array}{r} 3322 \\ \underline{4116} \\ 7440 \end{array}$$

也就是说,虽然写法各异,但这两种进位制中的运算结果是相同的,因为不同的数字系统只是表示数字的不同语言。数字间的彼此关系不依赖于数字系统。整数 10 在三进位制中就是 101,它也可以被 2 除尽,因为在三进位制中,101 = 12 + 12 = 2 × 12。

人们可以联想到其他的数字系统。例如某个行星的居民视 13 为基数,他们一只手有 6 个手指,另一只手有 7 个手指。

金星上的居民有多少手指?

马丁·加德纳因为在美国杂志《科学的美国人》发表许多趣味数学问题而出名,他曾给读者出过如下一个趣题[①]:一架在金星表面软着陆的宇宙探测器用无线电向地球传回一个悬崖峭壁上的图案。下面就是被刻在悬崖上的符号:



显而易见,这是金星上居民记录的加法,看来他们采用了一种和我们类似的数字系统。如果他们系统的基数由一只手上手指的数目而定,试问金星上的居民每只手有几个手指?

两指世界的演算

如果利用电线作为数字载体,则二进位制显得异常重要。我们已了解莫尔斯电码只认识长和短两个符号。

只有两个手指的生物不是0、1、2、3……,9、10、11、12,而是0、1、10、11、100、101、110、111、1000、1001、1010、1011……这样计数。8在两指世界中被写成1000,因为$1000 = 2^3 = 8$。这和我们把1000写成一千没有两样,因为1000是10^3。现在我们进位制中的1764在二进位制中看上去怎样?注意:$2^1 = 2$,$2^2 = 4$,$2^3 = 8$,$2^4 = 16$,$2^5 = 32$,$2^6 = 64$,$2^7 = 128$,$2^8 = 256$,$2^9 = 512$,$2^{10} = 1024$。

于是得出$1764 = 1 \times 2^{10} + 1 \times 2^9 + 0 \times 2^8 + 1 \times 2^7 + 1 \times 2^6 +$

① 《数学魔术》,柏林,1988年,第107页。

$1\times2^5+0\times2^4+0\times2^3+1\times2^2+0\times2^1+0$。

1764 被换算为二进位制中的 11011100100。乍一看，这比我们原来的写法繁琐得多。但是这样人们可以让每根电线在瞬间传过 11011100100。让我们再次练习二进位制中的演算。例如 7 + 13 = 20。在二进位制中，$7=1\times2^2+1\times2^1+1$，就变为数字 111，13 变成 1101。把两数相加，注意 1 + 1 = 10，则：

$$\begin{array}{r} 111 \\ \underline{1101} \\ 10100 \end{array}$$

最后的数字意味着 $1\times2^4+1\times2^2$，这就是 16 + 4 = 20。演算不取决于采用哪种数字系统工作。

两个二进位制数字相加时，如我们列举的二进位制数字，我们的方法和十进位制的加法时一样。一旦两个数字之和大于 10，那么在十进位制中，我们就要做十进位。相应地在二进位制中，一旦两个数字之和大于 2 就要采用二进位。鸭舍的居民演算时实行八进位。

但我们在十进位制领域中也了解了没有十进位的加法。虽然这提供的不是一种加法的结果，但它从明文数字和密钥数字的两个数字中产生出第三个数字——密文数字。R·佐尔格的报务员是这样相加的，同样的我们已在 143 页演示过。我们此时相应地在二进位制做没有二进位的加法。刚才所举例子结果如下：

$$\begin{array}{r} 111 \\ \underline{1101} \\ 1010 \end{array}$$

1 1 1
2
3 3
4 4 4
6 6 6
8 8 8
0 0 0

这是十进位制中的10。这种没有二进位加法的奇特方式得出的不是本应为20的数字和。但它从两个数字中得出第三个,就如由明文数字和密钥数字产生密文数字。一位年轻的美国工程师于1917年就注意到这一情况。

电传系统中的密码

吉尔伯特·S·弗纳姆在美国电话电报公司(AT & T)的一个部门工作。当初这一领域的重大新事物就是可打印的电报机。从这台机器内出来的不再是一长串点和线的条带,而是一段由电动式打字机打出的完整文章。今日的电报业仍然运用这一原理。纸带操纵电动机器,纸带上面冲出5排小孔(图11.2)。

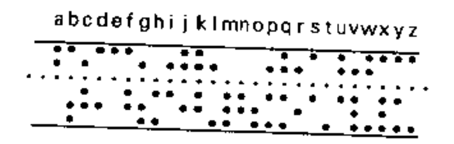


图11.2:电报系统中通过在纸带上冲出的孔和空格表示字母、数字和符号。水平延续的小孔是用于传送纸带。如果条带在金属底座上穿过电报机,5个电动探测器探针便探测纸带。一旦它们扫过一个孔,一个电的接触点被关闭。

这种密码可以追溯到法国发明家J·M·E·博多。每个符号对应着纸带上冲出的5排小孔和未冲出的空格组合,它被一排小孔隔开以传送纸带穿过机器。运用这种方式可以表示出二进位制中的所有字母,数字和标点符号。《浮士德》中,歌德的魔法两数乘法表也适用于此:小孔表示1,空格表示没有。因此字母a在纸带上被打印成孔－孔－传送孔－空格－

空格-空格形式或者二进位制的数字 11000。与此相对的字母 Z 即为 10001。

以此就可以加密。我们列举一个明文字“rose”(玫瑰),它被打印成 01 010 00 011 10 100 10 000。我们又选出 HUND(狗)为密钥字,它在电报条带密码中被表示为 00 101 11 100 00 110 10 010。如图 11.3 所示,把两个数字按照没有二进位加法相加得到密文。破译者从密文中又减去密钥重建明文。

明文: 01 010 00 011 10 100 10 000
密钥: *00 101 11 100 00 110 10 010*

密文: 01 111 11 111 10 010 00 010

图 11.3

弗纳姆制造了一台机器,它能逐个字母地同时读出两条纸带。各条纸带都载有上述五码中的孔和空格,其中一条载有明文,另一条载有密钥。当机器同时探测两根条带时,它在第三根条带上冲出密文。明文为一,密文空格,或者两者颠倒一下,每次就冲出一个孔。如果条带在相应处都有孔或都是空格,那么就不会冲出孔。

这和二进位制中的没有二进位的加法完全一致。因为 0+1 和 1+0 都得 1,0+0 和 1+1 的结果却为 0。脱密时,机器必须从密文中减去密钥,相应的规则为 0-1=1,1-0=1,0-0=0 和 1-1=0。通过一个合适的电路,根据这些运算法则,它或者冲孔或者形成空格,又得到二进位制的明文并让打字机打出。

发射台和接收台必须拥有相同的密钥条带。起初,AT &

T的工程师们把密钥条带首尾相贴成条带。由此，他们得到的是一条自行重复的密钥。这种密码可用于解开卡西斯基的维吉尼亚密码相同的方法破译。虽然机器密码简化了加密和脱密。但只要使用的条带不是特别长，密码的安全性就未得到提高。差不多在欧洲研制出一次一密乱码本，一种无限长的绦虫式密钥方法的同一时刻，以弗纳姆为核心的工作人员采用特长纸带作为密钥。这种操作方法没有成功，而弗纳姆则属于密码业众多发明家的一员，他们尚未施展才能就已离开人间。

第二次世界大战爆发前不久及随后的日子里，弗纳姆原理在德国也获得新生。1941 年，德国人启用了一种新型密码机，由洛伦茨公司制造的 S240 和 S242 规格的密钥附属装置。在博多电码中，明文被冲在穿孔带上。输入时，博多电码 5 个洞行的每一个都被探测。每行的信号孔(1)或空格(0)各从两个密钥轮上经过，这样进行一次加密。也就是说，有 10 个密钥轮。它们中的每一个在外部都载有一定量的销钉，一个密钥轮大约有 23 个销钉，另一个有 59 个。加密如是进行着：销钉保持原来的位置不动，这表示一；或者被击下，这表示零。在弗纳姆那儿，5 排孔的每一处被电子触摸，而且其结果在一条电路中(孔或者空格，即一或零)被与密钥条带的相应位置进程比较。此时把它和密钥轮当前的位置连接起来。明文条带的所有 5 排孔的结果都以孔或空格形式被记录在一条新的已被冲出孔的穿孔带上。这根新条带就含有密文。如果要读出明文 5 码组并冲出密文，这 10 个轮子以一种特定的、但无规则的方式继续转动。

最高领导层交换消息时采用洛伦茨密钥附属装置加密的密码，例如希特勒大本营和散布在全欧的总参谋部之间往来

的消息就这样加密。

布雷契莱庄园除了致力于破译“恩尼格玛”机电报外还必须研究德国人的密码技术。不管这个体系如何巧妙，英国人也能破译。不过普通型“炸弹”机对此力不从心。于是诞生了新型的，更有成效的机器，首屈一指当推“巨人”计算机。“炸弹”机仍属于机电式机器，其中电磁铁驱动轮子，检验继电器，看是否有一个“筛子”导向可能的日密钥，尔后止住马达。而“巨人”则与此相反，它属于电子式机器，即开关电路储存数据，规定运算的节奏，并检验二进位制中储存的数据是否与别的一致。第一台“巨人”机器装有 1500 根电子管(1948 年才发明晶体三极管)，后来的型号配备了 2500 根电子管。

我们当然不能依赖一根带有小孔 - 空格电码的条带来标明二进位制中的数字。电子脉冲同样能在二进位制中以脉冲及脉冲中断的节奏顺序任意传送篇幅很长的消息。它们能被以磁性格式储存在磁性条带或计算机的硬盘上。人们可将电子开关组拨至“开”或“关”处，由此储存二进位数。计算机为密码学指引了一个新方向。

DES——美国的标准系统

1977 年，美国政府启用一种新型密码系统——数据编码标准，缩写为 DES。它也许是目前使用频率最高的一种系统。按照他们完整的说法，只有经美国政府许可才可完整地使用这项发明。DES 最初是由 IBM 公司研制成功的。直至今日还无人在不知密钥的情况下成功破译用 DES 加密

的信息。[①]

对 DES 异常复杂的操作细节感兴趣的读者可参阅以下框内所做的简单说明。

DES 模式

在 DES 系统中，明文被写成二进位制数并被分成六十四个数字的信息组，即为链式的 0110011010100011010 01……形式。计算机工作人员称这种六十四信息组为位(Bits)。每个信息组从属于一个复杂的程序。此处约略提及就够了。

发送台和接收台都有一个密钥，一个 64 位的信息组。DES 程序由此产生 16 个 48 位长的子密钥。此外这个程序还包含一个子程序，它能把一个 32 位长的信息组和一个已被提及的子密钥联接起来，由此产生一个 32 位长的信息组。但这只是准备工作。

此时 DES 程序把每个 60 位长的明文信息组分解为左右两组，各组都是 32 位。尔后，这两个信息组各转 16 圈。并一再与 42 位的子密钥发生联系。最后它们被混淆得不可分辨，而且运用子密钥把组合的两半又变为一个 64 位的信息组。现在这就是密文组。破译者只有知道密钥把各个步骤倒退回去才能顺利得到原先的信息组。

然而就是这种程序还太简单。因为每个 64 位长的信息组都按同样的方式加密，相同的明文也提供相同的密文信息组。在某种意义上，这种操作程序还是单码循环加密。如果多篇明文都以同样长的文本开头，例如地址或称呼，那么密文也以同样的信息组开头。因此这 64 个信息组只有在最简单的 DES 操作程序中，按照所谓 ECB 方法逐个进行加密。按照更巧妙的方法，信息组在加密时也还是这样相互联接，同样的明文组不会提供相同的密文组。尽管起初的 ECB 方法有不妥之处，但美国的 DES 使用者依然对它满意。[②]

---

① 人们在 W·W·普雷斯、B·D·弗兰纳里、S·A·陶克斯基和 W·T·维特林所著的《数字化方法》(剑桥，1986 年)一书中能找到每一个 FORTRAN 和 PASCAL 程序设计语言的简化程序样本。

② 菲利普·齐默尔曼：《PGP(tm)用户指南》，第 1 卷，此为 PGP 程序使用指南(附录 D)，已附在程序中。

计算机进入密码领域使加密巨大数据量成为可能。原则上每个人都能轻易地利用个人电脑加密自己的信件。这引起国家的注意。按老的惯例,国家采用密码形式不仅侦查敌人,而且还有盟国的情况。但是它的公民可以向它们保守任意多的秘密,这是前所未有的。我们越来越多地通过远距离通讯渠道以电子方式转移货币。为使诸如此类的金融交易顺利进行,就必须传送加密指令。通过因特网订购货物的顾客不愿第三者知道自己的信用卡号,甚至密码。在电脑上利用电子银行从帐户上取钱的人不愿外人知道自己帐户上的金额。通过电子交换的信息愈来愈多,对密码的需求也在不断增加。国家对此会作何反应?

密码和政府

在任何时候,这个世界上的强国都使用密码。他们彼此交换加密的信息并破译他国的信息,为的是从中获益。

1628 年,胡格诺派教徒控制了法国南部城市雷亚蒙特,但是却被国王的天主教派的军队重重包围。防御者从钟楼上用一门大炮开火射击,看上去他们决不弃城。但是包围者逮住一个信使,他把一封加密信息带给在周边国的胡格诺派军队。一位被紧急招来的业余密码学家不费吹灰之力就破译了密码。内容是迫切请求增援弹药,因为大炮几乎射完所有的炮弹。包围者未加评论把明文还给发信人。他们随即投降。

这位破译者还年轻,名叫 M·安托万·罗西格诺尔。他后来成为那个时代最伟大的密码学家。不久之后,红衣主教黎塞留包围了拉罗谢尔城内的胡格诺派教徒,同样也截获一份

加密信息，他召来罗西格诺尔，他同样破译了这封信。包围者因此获悉城内饥荒严重，人们迫切等待英国船只从海上运来的食物。黎塞留此时只需封锁港口。一个月后，城市投降。

尔后，国王路易十三雇用罗西格诺尔。宫廷及其行政机关以加密的形式通信，罗西格诺尔为这种信息交换首次引入了分成两部分的术语表，即密码本的前身。国王如此宠幸这个密码学家，以至于生命垂危时还向宫廷官员们推荐他。太阳王就是路易十四，这位太阳国王，也喜欢利用罗西格诺尔的才智。他的威望、影响力和财富与日剧增。他第一个知道国家中发生着什么事情，他甚至比别人先知道国王的宠幸是哪个。路易十五也经常召来罗西格诺尔帮忙。

密码学不仅仅在法国宫廷受到重视，路易十五从维也纳发出的一包脱密信件，这是欧洲君主们寄给自己驻维也纳公使的信件，他大为惊讶。随后他看到自己的信件也被脱密为明文。奥地利秘密警察破译了所有这些文件。

当时欧洲各国都有自己的密码机构，即所谓的“黑屋”。奥地利人拥有最好最有效的“秘密内阁办公厅”。每天早晨7点钟左右，邮寄给各国大使的包裹抵达维也纳。公职人员小心地拆封并记下各页信纸顺序，以便以后能准确地把它再装入信封。他们大声朗读信件的内容，速记员笔录。尔后，又封上信件。9点半，外交包裹被送回邮局，10点正，它们和早晨的邮件一起被送到各国使馆。下午的邮件遭此同样命运。密码机构破译加密的信息。秘密警察工作效率如此之高，只有偶尔一两次把信装错信封。他们不仅这样处理外交信件，而且也这样处理嫌疑分子的往来信件。

有这样一个故事：一个人在信中告诉自己的朋友他在信

内附一只活跳蚤，以便检验途中是否有人拆开信封。事实上他并未在信内装入跳蚤。然而当他的朋友拆开信封时，一只跳蚤向他迎面跳来。维也纳黑屋的工作简直是十全十美。

到了现代，各国政府不仅试图读出敌对国家的加密信息，而且也想察知友好国家的加密信息。美国有一次暂时的例外。1929年，新任国防部长的亨里·L·史汀生呼吁："一个绅士不看他人的信件！"并取消了对美国"黑屋"的财政津贴。于是军方设立了以当时最伟大的密码学家威廉·弗里德曼为首的密码机构。

今日的美国拥有强大的国家安全局(NSA)。我们在图4.3中已见识过它的图章。它是1952年由当时美国总统哈里·S·杜鲁门创立的，多年以来，它的存在一直是个秘密。它窃听可能威胁美国安全的各国情报，破译加密的消息。大约有4万名工作人员为之服务，其中云集的数学家比世界上任何其他机构都多。

NSA也监督密码系统的出口。美国密码学家菲利普·齐默尔曼这样谈到："NSA参观了美国所有生产密码程序的公司，在密谈中建议他们降低程序的保密性。"[①] 美国的出口法规定禁止向外国出售密钥长于40位的密码程序。NSA自认为凭借其在计算机和密码学家方面的潜在优势能够破译这样的密码。这种推测容易理解。

1997年2月，报刊传播了一条新闻：一位年轻的苏黎世信息学家成功地破译密钥为48位的程序。无数计算机通过因特网投入了使用。

① 《明镜》周刊，1996年36期，第201页。

许多西方国家的秘密警察受到怀疑，故意对密码系统做了手脚后卖给其他国家，如卖到中东。因此，一家向伊朗、伊拉克和利比亚提供密码服务的知名公司据说在机器内装入小部件，它们用其制作的密文偷偷带入对所用密钥的提示。美国显然在繁多的政治局势中掌握它只有通过私自脱密得来的情报。有迹象表明 NSA 也能进入世界各国银行间的数据库。很可能以这种方式可以追踪毒品交易商的金钱流向。但我们能保证美国经济通过破译欧洲加密的信息往来而没有从中获益？就连欧盟各国也并非一直互相信任。当韩国购买一种高速列车系统时，《明镜》周刊① 写道："ICE 交易的失败使经营者们还沉湎于痛苦的回忆之中，在韩国举行的谈判中，法国的竞争者以万分的自信报出最低的价。现在技术人员排除了康采恩计算机网络中的信息漏洞。"

早在 1987 年，理查德·J·波利斯，这位日内瓦的一家致力于保护电子数据公司的创建人断言，为了非法获得客户数据，政府机构频频入侵银行网络。他写道，首当其冲的是美国政府。它一再企图侵入欧洲银行网络。② 只有对数据进行大量安全的加密才能对付这一不良行为。

密码不仅有助于避免有人非法获得与他毫无关系的数据，而且可使每位公民能与他人交换秘密信息。一些人认为这是公民的正当权利，比如本章开头援引的作者菲利普·齐默尔曼，PGP 密码程序的发明者，就是其中之一。但是丈夫和情人能借用密码交流信息，这也许给家庭生活带来伤害，而不会

---

① 《明镜》周刊，1996 年 36 期，第 195 页。

② "欧洲人的需求和对信息秘密的态度"，《密码学》，1988 年 10 月，第 134 页。

让我们国家的公益遭受侵害，犯罪组织和与国家敌对的组织也能使用密码。因此毒品黑手党就能从哥伦比亚出发借用因特网安排下一批货的运输路线，而右派或左派恐怖分子则能从网上获悉下一次聚众闹事的时间和地点。

1996年末，联邦宪法保护局局长彼得·弗里施在一次采访中警告："在因特网中，任何人都可以浏览到新纳粹分子的宣传以及左右翼极端分子指导制造武器的说明。"[1] 弗里施建议起草一部密码法，能使安全局在电子数据网络中阅读加密信息。

所有的数据监护人和那些认为上次的人口统计就已侵犯他们隐私的人们全力反对。我对此事不能理解。我曾在两种专制制度中生活了10年并懂得珍惜自己差不多已享受50年的民主，尽管它也有诸多内在的不尽如人意之处。因此我愿意授权予它在理由充足的条件下监督加密的信息往来，比如谁必须通过因特网传送加密数据，例如银行可以把密钥交存在一个联邦机构处，而一个特别委员会则监督国家不得滥用这种特权。

然而人们对此意见不一，正如每个人可以想象的那样，他们只能在边上注视就所谓大规模进行窃听的讨论。本章开始两段引言表明，即使在美国，人们对此观点也不一致。

目前德国并不禁止互通加密信息。密码在德国被视为一种武器，使用它要得到特别允许。[2] 在美国允许任何人加密，与此相反的却是限制其出口。而在俄罗斯，没有国家的特许，

---

① 《格丁根日报》，1996年12月8日。

② 克劳斯·舍恩莱伯：《个人电脑数据的加密程序》，波英，1995年，第181页。

根本就不能加密。

70年代末,一种全新密码原理被发现后,关于加密信息的争论已达到白热化程度。

12

公开加密

我们生活在这个地球上为数不多的一个国家中，在这里，人们可以通过承认缺乏数学才能而改善他的社会地位。

——瓦尔特·克雷默尔《思考！》

我们一再听说的这个观点肯定是错误的：几个世纪以来，数学家们都在寻觅因子分解法[①]，迄今尚未找到快捷的算法。所以人们必须正视其困难性。直到出现了计算机，才发现了发挥其优势的算法，以前只是用笔和纸加快计算的速度。

——约翰内斯·布赫曼《大数的因子分解》

我们早已习惯接受这样的事实：如果魏斯先生和施瓦茨女士想互通加密信息，在这之前他们必须交换密钥。为了从

① 因子分解法就是把一个数分解为因子的积。这是破译根据本章介绍的公开密钥法加密的最重要的辅助手段。

密文复现到明文,即使是凯撒也必须事先通知收信人把字母表推移几个位置。利用维吉尼亚密表加密的人必须让收件人知道密钥字。和整篇明文一样长的密钥字系统,如一次一密乱码本系统,虽然保证未经允许的人无法破译密文,但前提是他不知道密钥。迄今为止,我们了解的所有加密法中,发信人和收信人必须掌握密钥。第二章中关于隐匿法的例子以及偏勒·凡尔纳的移位法情况同样如此:双方需要同样的模板。即使它是随机产生,使用无限长的绦虫式密钥,他们也必须以同样的基数开始。无论如何都必须在传送信息前就统一密钥。

小密钥客户

让我们看一看一个简单模式中发件人和收件人存放的密码密钥的问题。密码密钥类似于我们日常生活中所用的钥匙。加密如同把一封信件藏在一只上锁的箱子里(图 12.1)。魏斯先生有这把锁的钥匙。他能用这把钥匙打开箱子并放入明文,就如一封信。一旦他把箱子锁上,大家再也看不到这封信,它变成密文。收件人施瓦茨女士同样也有一把能打开这只箱子的钥匙。打开箱子的刹那间,这封信不再是秘密的,它成为明文。借助于这把钥匙,施瓦茨女士此刻能阅读这封信。收件人和发件人都是拥有同样钥匙的平等伙伴。由于他们拥有完全一样的钥匙,我们称之为"对称的钥匙管理"。它是我们迄今遇到的所有加密法中的基本要素。发件人和收件人始终使用同样的工具。因此施瓦茨女士也能发信,而魏斯先生则收信。但必须有转交钥匙的时刻。这始终是个薄弱环节。

看起来有规律可循:想加密的人必须拥有也能脱密的密钥。但事实并非如此。用其他方法也行,只不过麻烦些。

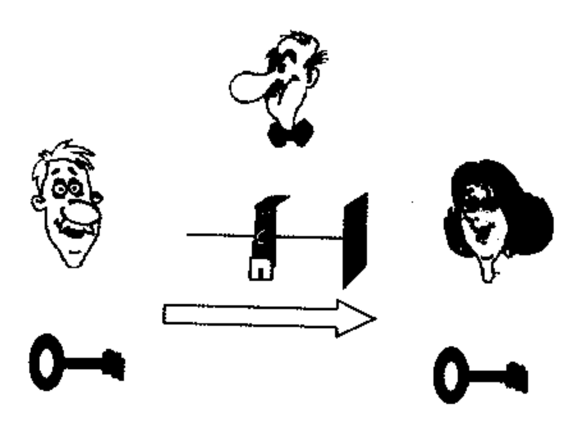


图 12.1:对称密码示意图。施瓦茨女士和魏斯先生各有一把钥匙能开启箱子上的锁。魏斯先生如果用钥匙锁住箱子,施瓦茨女士可用自己的钥匙把它打开。但其中一人必须在某个时刻从另一人手中接过原配钥匙的复制品。

首先我想用箱子、锁和钥匙这一简单例子阐述这个过程。魏斯先生想给施瓦茨女士发一封信。他有一只箱子、一把挂锁和一把相配的钥匙。施瓦茨女士也有一只配有钥匙的挂锁。两把钥匙均不能打开对方的锁。此刻,魏斯先生给施瓦茨女士写信,他把信放入箱内,挂上锁并锁住箱子。此时,上锁的箱子抵达施瓦茨女士处(图 12.2)。她根本不想打开魏斯先生的锁,因为她的钥匙不配。她拿出自己的锁取而代之,也把它挂在箱子上并同样锁上箱子。此时这只被双重锁住的箱子又回到魏斯先生那儿。他打开挂锁并取下锁,把箱子又送给施瓦茨女士。这只第三次在途中运行的箱子此时还被施瓦茨女士的锁锁着:但她能用自己的钥匙打开自己的锁,终于取出这封信。她大声地读道"早晨 3 点钟"。传送这样一份微不足道的信件的程序竟是如此繁琐复杂。但是他们都不必交出自己的钥匙。在运输过程中,这只箱子始终至少被一把锁锁

住以保障安全。未经允许的格劳先生没有机会打开箱子。

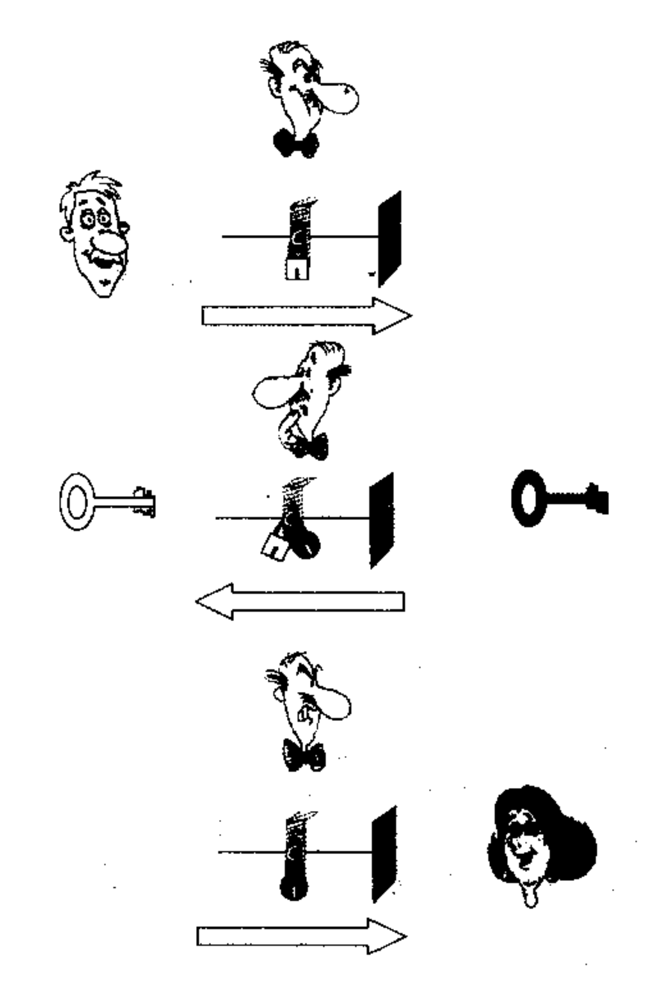


图 12.2:无需交换钥匙的对称密码示意图。施瓦茨女士和魏斯先生各有一把锁以及相配的钥匙。魏斯先生用自己的锁锁住箱子,把它送给施瓦茨女士。她把自己的锁挂到箱子上并锁住把它交还给发件人。魏斯先生取下自己的锁,又把它再送给施瓦茨女士。此时她可用自己的钥匙打开箱子。这两人之间不必交换钥匙。

利用箱子、挂锁和钥匙可以这样进行,但在密码学中又是怎样的情形呢?我们假设:魏斯先生的密钥一直是《苏菲的世界》的开头:SOFIEAMUNDSEN……,或者用数字,如果我们以它们在字母表中的号码代替字母,

S O F I E A M U N D S E N W A R …
19 15 06 09 05 01 13 21 14 04 19 05 14 23 01 18 …

而施瓦茨女士此刻也有自己的密钥,是弗里德里希·迪伦马特所著的《法官和刽子手》的开头:"Alphons Clenin, der Polizist von Twann……"。密钥字以数字反映即为:

A L P H O N S C L E N I N D E R …
01 12 16 08 15 14 19 03 12 05 14 09 14 04 05 18 …

魏斯先生取出明文,按同样的原理把它转变为:

m o r g e n u m d r e i
13 15 18 07 05 14 21 13 04 18 05 09

尔后,他利用164页中介绍的没有十进位的加法法则加上密钥进行加密(图12.3A)。他把数字结果送给施瓦茨女士,她取出自己的密钥,同样按着没有十进位的加法法则作加法(图12.3B)。她把这结果交还给魏斯先生。他(从中)减去自己的密钥(图12.3C)。此时这一结果又送到施瓦茨女士处。它目前还被施瓦茨女士的密钥锁着。她取出密钥得到明文(图12.3D)。他们中无人必须知道另一人的密钥,而信件在交换过程中始终处于加密状态。格劳先生又无机可乘了。

这种不交换密钥的加密法只有在发件人和收件人相互交换密码的条件下才有效。如果魏斯先生和施瓦茨女士先后用

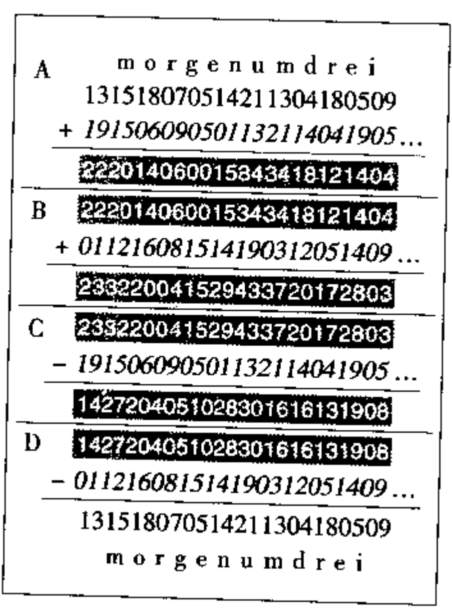


图 12.3:交换无需互通密钥的加密信件。A:魏斯先生的明文,用数字表示的明文和密钥文。横线下是(通过没有十进位的加法)得到的密文。B:刚才产生的密文第二次加密,此次用施瓦茨女士的密钥。C:魏斯先生又减去密钥。此时的明文还被施瓦茨女士的密钥锁着。D:施瓦茨女士再减去自己的密钥,这样出现明文。在此过程中不必互换密钥。

自己的密钥加密,同样的密文就以相反的次序出现。此处选择的加密程序就是这种情形。如果与此相反,每人使用单码密码和一个已排列过的字母表,而且每人用另一个密码,那么这个被阐述的程序在破译时会使字母产生混乱,因为两次排列的结果取决于它们的顺序。

实际操作中存在着更简单又更重要的加密法。它们不要求互换密钥。让我们再看一遍我们的模式。现在,我们设想一把有 3 个钥匙孔的锁和相应的 3 把钥匙(图 12.4)。我们有一把大钥匙 N 和两把小钥匙 E 和 D。每一把钥匙都有一个相

配的钥匙孔。想上锁的人必须用一把大钥匙和其中一把小钥匙,例如N和E。但无法再用它们打开锁。如果用N和E锁住,只能用N和D打开,反之亦然。现在,我们借用这把神奇锁让施瓦茨女士和魏斯先生在箱内交换密信。

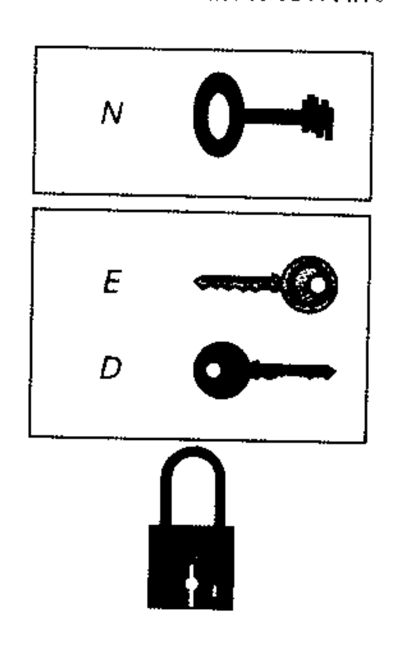


图12.4:锁和钥匙是例子中非对称加密的工具。这把锁有用N,E和D标明的3个钥匙孔。开和关都必须使用大钥匙N和两把小钥匙中的一把E或D。如果用N和E上锁,必须用N和D才能将其打开。

施瓦茨女士从一家使人信赖的公司那儿得到这把锁和3把钥匙。她让人复制了许多把N和E,把它们分送给朋友和熟人。格劳先生也有一把,它们是人手一把的"公共钥匙"。但是施瓦茨女士自己留存钥匙D。这是她的"密钥",没人(包括魏斯先生在内)拥有这把钥匙D。她把三孔锁挂在箱上。每个想给她发密信的人都可拥有这只箱子。

我们此时让图 12.5 中的魏斯先生给施瓦茨女士发一份密信。他拿起他的明文放人箱内。然后用施瓦茨女士的公共钥匙，即 N 和 E，锁上箱子。从此刻起，他再也无法取出箱内的东西。这只被钥匙 N 和 E 锁住的箱子只能用 N 和 D 打开，除了施瓦茨女士，没人能开启箱子，因为只有她有钥匙 D。醋意大发的格劳先生也无法夺取箱内的东西。此时与那只有两把同样钥匙的箱子不同，魏斯先生和施瓦茨女士已不再有同样的工具。魏斯先生有施瓦茨女士的公共钥匙，可是城内的每个人都有这两把钥匙。而施瓦茨女士有一把其他任何人都没有的钥匙。此时的这种情况不再是对称，人们称之为“非对称钥匙管理”。

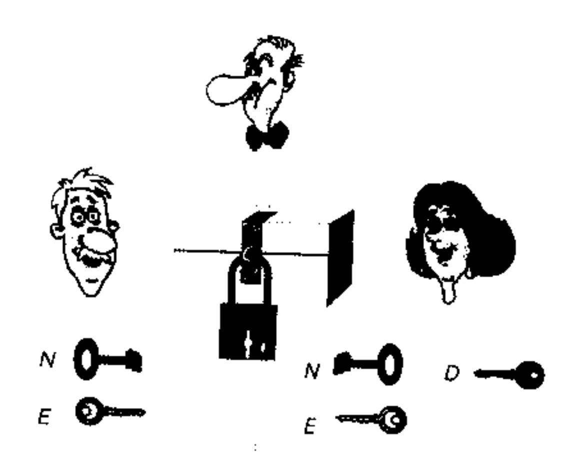


图 12.5：一种非对称加密示意图。图 12.4 的锁挂在一只箱子上。施瓦茨女士有 N、E 和 D 3 把钥匙，她把复制的 N 和 E 分发给所有的朋友。但她留存钥匙 D，除了她没有人再有 D。当魏斯先生想把箱内的密信交给施瓦茨女士，他用钥匙 N 和 E 锁上箱子。尔后，他自己也无法再打开箱子。只有施瓦茨女士用钥匙 D 才能取得箱内密信。

密码学中也可利用公共和秘密密钥发送信息，因为存在

着无需约定的共同密钥的操作方法。在此方法中,数字起着非同寻常的作用。因为这不再是明文和密文交换,而是明文数字和密文数字交换。

从明文转换为明文数字并非难事。每个明文字母被字母表中的序号代替。也可根据波利比乌斯表进行转换。为简便起见,我们采用字母在字母表中的序号。我们再次举“rose”这个词作为明文,其相应的明文数字是 8 位数“18151905”。它要变换为密文数字。怎样换算,且看分解,收件人必须采用另一种换算方法把它变回明文数字,他再次用明文字母代替明文数字对。秘密就在于从明文数字到密文数字以及相反的换算当中。

非对称法加密的食谱

食谱中标出原料的分量,我们从中可以准备一道菜。取 125 克麦糁,半升牛奶和 30 克黄油以及其他相关的原料。不必问为什么放入 30 克而不是 80 克黄油,或者这道菜中为何不撒入 300 克火腿丁。但愿作者已试着烧过这道菜。就魏斯先生怎样把密信交给施瓦茨女士,而两人事先并未商议出一个密钥这一问题而言,我们同样只研究食谱而不解释为什么。

取两把钥匙,我们称大的为 N,两把小的分别为 E 和 D。这些钥匙应是数字。但是我们也能把它们想象为如图 12.5 中的真正钥匙以便阐述。取一简单例子:假设 N = 85, E = 5, D = 13。这并非是我随意杜撰的 3 个数字。它们之间确实存在着一种特殊关系,这并非马上会让人注意到。N 为 33, E 为 3 和 D 为 7 之间也存在这样的关系。我们称这样的数字为“幻数”。N = 20, E = 11 和 D = 5 就不能构成幻数。人们怎样找到

这3个幻数，附录C中会作说明。例如N = 49048499，E = 61和D = 2409781也是幻数，实际运用中需要更大的数字，那些带有多于100个十进制数位的数字。就食谱而言，我用了较小的数字，N = 85，E = 5和D = 13。施瓦茨女士和魏斯先生把这3个幻数作为密钥。施瓦茨女士必须像爱护自己的眼睛保护E或D，我们认为保护D。她不向任何人透露这个数字。如果数字太长，她必须记下这一数字，并把它放在保险箱内的首饰旁。当施瓦茨女士把D作为秘密守护时，她可以公开E和N，并在明信片上通告："所有愿意给我写信的朋友可以用我的公开密钥数字N和E(即85和5)加密信件。"

魏斯先生也得知此事。一般情况下，他写篇幅较长的信件，诸如："你觉得昨晚的音乐会怎样？"为简便起见，我们假设今天他的明文只有一个字母，如X。这封信的内容毫无大肆渲染的价值，但我们可以用它来认识原理。字母X在字母表中对应的数字是24，这是明文数字。此时魏斯先生可以加密。他知道公开密钥为N和E，他无需知道更多的东西。另外，施瓦茨女士还掌握着D，但这和魏斯先生无关。

利用N和E加密

写下E这个明文数字并进行乘方运算。在乘出时，只要可能，在有中期结果时就不断减去N，以使这数字不会太大。最后剩下一个小于N的数字，这就是密文数字。

用N和D解密

写下D这个密文数字并进行乘方运算。在乘出时，只要可能，在有中期结果时就不断减去N，以使这数字不会太大，最后剩下一个小于N的数字。这就是明文数字。

魏斯先生加密,施瓦茨女士脱密

这个烹调要求魏斯先生取明文数字(即 24)去乘 E(在此为 5 次幂),即计算 $24^5 = 24 \times 24 \times 24 \times 24 \times 24$。他根本不需要这个数字,而仅需要它除以 85 剩下的余数。如果他不怕数字大,他把 $24 \times 24 \times 24 \times 24 \times 24$ 得 7962624,再把这个数字除以 N(85),这道计算题并未被除尽,而是留有余数。这个余数即为密文数字。如果您复算一下,得到的乘数是 79。79 就是密文数字。

在处理真正大的数字时,在有中期结果时不断减去 85,正如上面的方框内建议的那样。起决定性作用的余数不会再变化,但中期结果很小。在下面的方框内列举了决定余数的较完美的办法。

无论魏斯先生如何计算,他得到的密文总是 79。他落落大方地把它寄给施瓦茨女士。其他人对这个数字束手无策。未被允许的格劳先生也是如此,因为他不知道密钥 D。但是格劳先生也能把一份密信寄给施瓦茨女士。他也知道她的公开密钥数字 N 和 E 并以此确立密文数字。魏斯先生也无法阅读,他甚至再也无法把自己创造的密文数字还原为明文数字,正如他无法从图 12.5 中自己上锁的箱内取出信件一样。

施瓦茨女士收到密文数字 79 后,充满期待地开始脱密。她首先从保险箱内取出密钥 D,即数字 13。然后计算 79 的 D 次幂(即 13 次):即 79^{13}。这是一项艰难的任务,因为结果是一个 25 位的数字。幸而她能简化运算。她只需计算与 N,即 85,有关的余数。每次相乘的积除以 85,继而如方框内所处理的余数。最后得到结果是 24,这就是魏斯先生加密的明文

数字,它对应的字母是 X。

> **用袖珍计算机处理庞大数字**
>
> 施瓦茨女士用 79 乘以 79 得到 6241。用它除以 85 得到 73.4235。亦即 6241 中含有 73 次的 85。85 乘以 73 只有 6205。即用除法的余数为 36。在 85 的余数范围内 $79 \times 79 \equiv 36$(模 85)。然后她计算 $79 \times 79 \times 79 \times 79 \equiv 36 \times 36$(模 85),余数为 21,即 $79 \times 79 \times 79 \times 79 \times 79 \times 79 \times 79 \times 79 \equiv 21 \times 21 \equiv 16$(模 85),因此 $79^{12} \equiv 21 \times 16 \equiv 81$(模 85)。所以 $79^{13} = 81 \times 79 = 6399 \equiv 24$(模 85)。在余数范围内,施瓦茨女士可用袖珍计算机完成所有的计算。

这封信异常简短。魏斯先生该如何处理内容比较丰富的信件呢？他可以按如上所述加密各个字母。他把明文字“rose”转换为 4 个明文数字 18、15、19 和 05,并按上述方式加密各个数字,产生 4 个密文数字 18、70、49 和 65,他把 18704965 交给施瓦茨女士。她可以把这个数列分成两组,并用秘密数字 D,即 13,各个脱密。“rose”又在她面前绽放。

不过注意！在字母式密码中,对应每个明文字母的是一个被转换为密文数字的一个二位数。这和单码密码并无差别。每个明文字母 e 被转换为同样的密文数字对。格劳先生——E 和 D 与他有什么关系？——他可以像刚才破译单码密码那样,根据分析不同二码组的频率分布来破译密文。另外,这种加密法还有一个弊端。字母 a 对应明文数字 1。无论它乘以自己多少遍,1 还是 1。这意味着 a 永远是 a。倘若魏斯先生信中提到一次 a,格劳先生就可能猜到明文是 abrakadabra。不过,不交换密钥的加密法也并非如此简单。我选择了相对简易的密码,因为这样我们能停留在小数字上,而数字小时,这种加密法容易让人理解。

如果魏斯先生把数列 18151905——我们已知这是 Rose 的名字——理解为一个唯一的数字,即大约为一个 1800 多万的数字,他就有更好的可能性。此时,只有 N 大于密文数字时,我们研究的方法才能奏效。因此我现在选择新的幻数,即 N = 49048499, E = 61 和 D = 2409781。您无需操心我从何处找到这些数字,这在附录 C 中会看到。

首先让我们观察一下,如果我们面前有 3 个幻数,这个方法如何起作用?处理如此庞大的数字时,您不再可能借助袖珍计算机听懂我的话。注意:魏斯先生为了得到密文数字,他必须把他的明文数字乘 60 遍。施瓦茨女士为算出明文数字甚至要乘 200 多万次。当然这里出现的数字保持在一定限度内,因为他们只须在 N 的余数范围计算。我利用自己的电脑替您完成这项工作,在此不仅仅对明文字"rose",而且还用同样的魔幻三重数组对两个类似的字加了密。图 12.6 表明其结果。人们看到类似的字被转换为截然不同的密文数字,甚至是与单一字母 X 对应的也是一个 8 位数的密文数字。格劳先生对此会无计可施,他想不到 X。

$N = 49048499, E = 61, D = 2409781$		
明文字	明文数字	密文数字
rose	18151905	10697935
hose	8151905	32147069
hase	8011905	40486608
x	24	23985193

图 12.6:借助上述的幻数 N,E 和 D 加密更多字的 RSA – 密码。

如果魏斯先生想寄一封含有 100 个或更多字母的长信,

此时情形如何？我们假设他的信件由100个字母组成，即200个明文数字对。这样他必须有3个魔幻三重组数，N至少是个200位的数。我们只能借助计算机完成必要的运算。

施瓦茨女士和魏斯先生因此约定：原则上把信件划分为4组或5组，单个加密，即每组与上述“rose”一样加密。

他们加密和脱密时要对付的数字长度由N决定。即使一个单一的字母文本如X，在加密时也能产生一个如我们在图12.6所见的庞大的密文数字。如果已学会怎样确定幻数，我们也将讨论格劳先生是否能成功地了解加密的秘密这个问题。结果会表明，他相对容易破译小N密码。如果N大于100位数或者更大的长度，就困难些，甚至几乎不可能。此处描述的加密的秘密和数字的类型紧密相关。很久以来，数学家们认为这些数字虽然有趣，但对实际应用却毫无意义。

不能被分解的数字

从前，农民拥有一些牲畜。他们必须清点绵羊数以查清是否有羊走失，这样就有了整数的问题。谁结婚娶妻，还可以从女方的嫁妆中得到牲畜，他必须学会把两数相加。女儿出嫁，作为嫁妆的牛和羊和她一起进入新家。父亲必须学会减法。当他年迈考虑怎样公平地把牲畜传给孩子们时，必须学会除法。一位拥有12条牛的农民发现，如果他有2、3、4或6个孩子，他才能把牛平均分给孩子们，而他决无可能平分13条牛，除非他只有一个或有13个孩子。在这样的思维过程中，人们学会与整数打交道，并且明白它们不仅有大小的差别，而且还具备完全不同的特征。

整数间存在着错综复杂而又令人惊讶的关系很快被证

实。因此“数论”这门学科得到发展。它研究整数的规律性。浩如烟海的书籍和杂志刊登的文章表明整数世界多么丰富多彩。我们无法预料数论的研究何时接近尽头。

象棋就是从少数几个初始规模发展为一个巨大的知识领域的另一例子。象棋中只有少量规定,如何可以走棋和吃掉别人的棋子。但是从这些简单规律中繁衍出整本整本的对策。大师们的经典棋局一再被刊登在专业文献里。它们都是不折不扣的艺术品,有些还被冠以相应的名称,例如 19 世纪中叶,布雷斯劳文科中学数学教授阿道夫·安德森赢的那场“不朽的棋局”。这些杰作也只是运用“卒走直线吃斜子”这些简单规律的结果。

象棋中并没有普遍的理论,而这项和整数打交道的游戏却被固定的原理操纵着。我们在第四章中已认识余数的计算。这是数论的一个分支领域。人们可把数字相加,相乘。在它们的余数领域内,它们的余数又可自行相加或相乘。这已是数论中的一个定律,虽然它非常简单。下面我将阐述它的另--分支领域——素数理论。它在加密中的作用重大。

我把两个整数相乘,得到的还是一个整数,如 10 乘 13 得 130。也就是说,我可以用 10 除这个数,它被除尽。用 2 或 5,或 13 除时也没有余数。130 和 10 是由 2 和 5 组成的合数。但 13 不是,它没有除数,是素数。13 当然可以被 1 和自身整除,但我们不考虑这两种简单的情况。2 和 3 都是素数。与此相对,4 有除数,而 5 没有除数。我们已有开头的几个素数:2、3、5。除 2 外,所有的素数都是奇数。当然是这样,否则它们可把 2 作为除数。图 12.7 中列出了 2 至 1013 的素数。在 1013 处打住的素数还能任意排下去吗?是否存在最大的和最后的素数,它后面的每个数都可被较小的数整

除？希腊数学家欧几里得大约在公元前 300 年就给出答案：素数没有穷尽。因此我们明白，我们的素数表还可任意排列下去。

2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569	571	577	587	593
613	617	619	631	641	643	647	653	659	661	673	677
683	691	701	709	719	727	733	739	743	751	757	761
769	773	787	797	809	811	821	823	827	829	839	853
857	859	863	877	881	883	887	907	911	919	929	937
941	947	953	967	971	977	983	991	997	1009	1013	

图 12.7：至 1013 为止的素数。

为什么存在无穷尽的素数

我们假设有一个最大的素数，我们称它为 G。然后我们把所有较小的素数相乘，乘以 G 再加上 1。我们称结果为 Y。这个数字肯定大于 G，因为 G 和所有的数相乘，另外还加上 1。它不可能被所有小于 G 的素数及 G 自身整除，因为所有较小的素数，包括 G，在做除法时得到余数 1。由此证明，要么 Y 自身是素数，要么能被大于 G 的素数整除。在这两种情况中都必须有一个大于 G 的素数。为什么存在无穷尽的许多素数，因为人们总能找到一个更大的素数。

筛选过的数字

我们现在如何寻找表格外的素数？另一位希腊人，昔兰尼学派的厄拉多塞，约在公元前250年发现一个简单的办法。他是著名的亚历山大图书馆馆长，又是第一个确定地球大小的人。他发现寻找素数的办法在今天被称为"厄拉多塞筛法"。

我们用他的办法确定第一个素数。我们在表内写下1至100的所有整数。现在从第二个数，即2开始，每隔一个数在下面划线。下一步从3开始，每隔两个数下面划线。已划线的数字也应考虑在内。当我们从4开始时，在从它开始的第四位数下面划线时，我们发现无需再划了，因为这些数在划2时已被划过横线。继续从5开始，在5后面的第五个数字下划线。从6开始时，我们不必操心了，因为这些数字已被划过横线。从7开始时，我们又会碰上没有划线的数字。图12.8表明结果。我们简单地思考一番，为得到小于100的素数，素数划线至多到7为止。与我们所列的素数表相比，我们确定没有被划线的数字正是100以内的素数。虽然1位于表格的第一位，但它并不被视为真正的素数，作为素数的它没有受到

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100					

图12.8：用"厄拉多塞筛法"确定素数。

认真对待。如果想找到更大的素数,我们一开始就写下一个更长的数列,并重新开始划线。

1903 年,最大的已知素数 2305843009213693951。以往人们只是零星知道这样庞大的素数,而美国数学家德里克·诺曼·莱默尔于 1914 年列出一张完整的表格,列有 10006721 的所有素数。图 12.7 所列的只是他那庞大素数表中的一小段。至 1996 年 11 月止,我们利用计算机发现的最大素数有 420921 位,但我们已经知道它还可以随意列下去。

9890601
9890623
9890641
9890643
9890661
9890677
9890689
9890697

图 12.9:根据莱默尔素数表所列 9890600 至 9890700 间的素数。

人们如果有一条按顺序列出所有素数的公式代替这费力的"筛子"该多好。下面的一条准则使我们对此充满希望。我用儿时的数字游戏来表达它:"想一个数减去 1,得到的结果和这个数相乘并加上 41!"您试一下,从 1 开始。得到的结果是 41,因为 $0\times1+41=41$——一个素数!由下一个数 2 得到 43,又是一个素数!由 3 得 47,由 4 得 53——又一个素数!但是与素数表相比,我们发现有些素数没有被表示出来。不仅缺少小于 41 的素数,而且也无法得到 59。如果这条规律没有反映出所有的素数,至少它能始终导出一个素数吗?我们取 12,结果是 173,素数。现在取 20,得

到 421，同样是素数。继续取 30 和 40，得到 911 和 1601，又是两个素数。

我们已掌握素数的世界公式吗？失望从 41 开始，它提供的结果为 1681，倒霉，这不是素数，因为 1681 = 41 × 41。世界上并不存在能按顺序计算出素数的公式。

小于 100 的数中存在 25 个素数。但在 900 至 1000 之间同样大的范围内只有 14 个素数。数字往上，素数密度递减，这是无规律的。500 至 600 间只有 13 个素数。人们发现在 1000 万的范围内，在 100 个不断的数字中大多少于 10 个素数。9921400 和 9921500 之间只存在 6 个素数。9893200 和 9893300 之间竟然只有 3 个素数。19 世纪，数学家们发现这个规律，据此在素数范围内，越往上，越难找到素数。但这条规律并未告诉我们哪些数是素数，哪些不是。

在素数分布中还出现一些奇怪的现象。让我们再一次观察图 12.7 的表。表中反复出现只差 2 的连续不断的数字。它们无法再贴近了，因为在两个仅相差 1 的数字中，一个是偶数。如果这个数不是 2 本身，那它就不是素数。如果两素数之差恰恰为 2，我们称之为“孪生素数”。我们在图 12.7 的表中发现有 2 \ 3，5 \ 7，11 \ 13，17 \ 19，人们可能以为，这与数字较小时出现的一种现象有关。素数较密集地连续出现。但是我们的表在 800 至 900 间列出了孪生素数，821 \ 823，827 \ 829，857 \ 859 和 881 \ 883。就是在 100 万范围内也出现孪生素数。图 12.9 中从莱默尔表中摘取的一小段中也有数对 9890641 \ 9890643。人们最近发现的一个孪生素数，其中每个素数都有 11713 个十进制数位。看来孪生素数序列也是没有穷尽的。

尚未被研究的领域

我一再碰到一些人,他们虽然明白人们在自然科学领域中,如生物学或者天体物理学,通过研究可以不断汲取新知识,但是他们难以想象数学研究没有穷尽,每天都会出现许多新知识。就连整数,我们也尚未了解它的全部特征。这儿有一个例子:

1742 年 6 月 7 日,圣彼得堡科学院的会议秘书克里斯蒂安·冯·哥德巴赫在信中告诉莱昂哈特·欧拉一个关于素数的数学定理。但他无法证明其正确性。至今尚未有人成功地论证这个定理。人们因此称之为"哥德巴赫猜想"。它说每个大于 2 的偶数是两个素数之和。简单的例子如:20 = 3 + 17,24 = 5 + 9,872 = 199 + 673。人们无论取哪个偶数,至今尚未发现它不是两个素数之和。但这并不能排除什么时候有人找到一个偶数款款走来,哥德巴赫猜想并不适用于它,因此它否定了哥德巴赫猜想。

与素数相关的另一个疑难问题涉及到它的乘法。两个素数相乘不是一件难事。但是如果数字庞大,人们就无法从其结果中看出它是由哪些数字组成的。数字小时很简单。每人都知道 85 = 17 × 5。但是人们如何从 1009961 上看出它是由素数 997 和 1013 相乘得来的呢?数字 991849 和 49048499 也是两个素数相乘的积。您能猜出是由哪些数相乘的吗?两个素数相乘是容易,但是把结果分解为原始数字却是很难。没有人发现隐藏在庞大的 N 中的素数,魏斯先生和施瓦茨女士往来信件的加密就依靠了 3 个幻数的帮助。

人们实际上至今仍无法在遇到一个由两个素数相乘得到

的200位的数时，重建这两个素数。但是没人知道数学家在什么时候是否会发现一种方法，用它可以把庞大的数字分解为素数，而所花费的时间远远小于现在的时间。被想到的是一种新型的、完全按别的原理工作的计算机，人们称之为量子计算机，用它可以迅速分解庞大的数字。

倘若有这样的进展，那我们所描述的公开密钥瞬间就失去了价值。

素数密码

这一方法自1978年才为人们所熟悉。同年，美国一家有名望的专业杂志的2月刊中刊登了一篇文章[1]，这是由马萨诸塞州坎布里奇市麻省理工学院计算机研究实验室的三位科学家共同撰写而成。它论述了两个问题。

第一个涉及的问题是，人们怎样通过数据导线在寄发的文件上签名，使收件人相信这个签名确实可靠。人们在日常通讯中用手签名，每位收件人、个人或是财政局，可凭借以往的签名认出这是否属实。万不得已时，例如在法庭上，必须由专家对此作出判断。但是您有一次用打字签名。收件人不知道这个名字是否由您自己打上的。同样的问题也发生在您那些通过电报或因特网发送的文件中。我们来看一看三位作者是怎样解决这一难题的。

就第二个问题而言，他们指出，人们怎样交换加密信息而

---

① 罗纳德·L·里弗斯特，阿迪·沙米尔和莱昂哈德·阿德勒曼，《获得数字签名和密码系统的公开密钥的方法》。《ACM通讯》，第21卷，第2期（1978年），第120页。

不必交出密钥。我们最初研究这一问题是因为魏斯先生和施瓦茨女士使用的密码系统就建立在这一基础之上。撰写这篇划时代文章的三位作者是数学家罗纳德·L·里弗斯特，阿迪·沙米尔和莱昂哈德·阿德勒曼。今天，人们相应地以他们名字的开头字母 RSA 称呼这种加密方法。

RSA 加密法的依据是人们设法找到 3 个在前面被我称为 N、D 和 E 的幻数。RSA 小组建议如我在附录 C 中描述的那样确定这 3 个数。他们取出两个素数，p = 47 和 q = 59，把它们相乘得到"大密钥"N = 2773。[①] 然后他们选取 E = 17 并根据附录 C 所述方式找到 D = 157。他们为了阐述而采用莎士比亚借用朱利叶斯·凯撒之口说出的名句

its all greek to me

作为原文，他们根据这些字母在字母表中的位置把它转换为明文数字，在各个字的间隙内插入两个零。他们这样得到被记为 4 个信息组形式的：

0920 1900 0112 1200 0718 0505 1100 2015 0013 0500

尔后加密回信息组。他们取第一个信息组数字为 E 次方，即第十七次幂。这样它们形成 920^{17}。每次相乘后只保留余数模 2773。最终结果是 948。第一个信息组如是被加密。由 0920 得0948。他们这样逐个地继续加密，直至完成任务。

0948 2342 1084 1444 2663 2390 0778 0774 0219 1655

① RSA 密码的实际操作中只有 E 和 D 被称为钥匙，而 N 不是。我在本书中把 N 也称为钥匙，因为打开锁的必要辅助工具毕竟被唤作钥匙。只知道 E 和 D 而不认识 N 的人就会站在被锁住的门前束手无策。

这就是密文。人们注意到 RSA 加密者并未利用数字 D。但这对于收信人而言,它是绝不可少的。

他通过取密文的各个四码信息组的 D 次方(即 157 次方)脱密,于是得到明文。这与 251 页中施瓦茨女士和魏斯先生在通信中使用的加密方法完全一致。

附录 C 表明,加密的秘密首先在于 p 和 q 的两个素数中,由它们俩得到 N。如果格劳先生能把公开的数字分解为两个素数,他就破译了密码。但是没有简单的方法告诉我们如何把一个约有 100 位的数分解为它的因子。因此,除了单调的试验之外别无选择。人们用 2、3、5、7、11……即小于 N 的所有素数除 N。① N 一旦被除尽,人们就知道这一个素数是除数。如果 N 庞大,这项运算就没完没了。

三位作者在 RSA 一文中估计把 50 位的 N 分解为素数必须计算 140 亿次。N 是一个 200 位数时,使用 1978 年的计算机运算,花费的时间像宇宙的年龄那样久。虽然在此期间,计算机运算速度加快,但是分解一个 150 位的 N 需要一个 40 位数的运算操作。——现在的计算机还无法跟上这一速度。

但是也还存在着易于分解的单个数字。1992 年,人们成功地分解了一个 157 位的数字。② RSA 使用者对这种例外数字当然只得不理睬。

90 年代初,坚信 RSA 的人大吃一惊。里弗斯特、沙米尔

---

① 人们无需取所有小于 N 的素数。只要试验小于 N 平方根的素数就已足够。如果在 0 和 N 的平方根范围内的素数不在 N 中,那它们也不可能是大于其平方根的数。

② 比 2 的高次幂小一点的数易于分解。1992 年,阿詹·雷斯特和丹·伯恩斯坦把 $2^{523}-1$ 这个数分解为两个素数。他们使用一台内含 16000 多个多重信息处理机的计算机运算了 3 个星期。如果 $(p-1)/2$ 仍是一个素数,素数 p 就特别适宜构成 N。

和阿德勒曼早在1977年8月就在学术杂志《科学的美国人》上刊登了一个129位的数字并愿奖赏100美元。谁想赢取这笔奖金就必须找到构成这个数的两个素数因子。这个数为：

$$N = \begin{matrix} 114381625757888867669235779976146612010218296721242 \\ 362562561842935706935245733897830597123563958705058 \\ 98907514759929002687954354 1 \end{matrix}$$

您当然必然考虑把所有这些数字连续写下。如果有人收到用N和E加密的信息，而N正是上面所举的129位数。只要构成N的素数未被知晓，密文就永远无法被破译。16年过去了，还未有人动过这100美元的奖金。

1992年，四位数学家攻克了这一难题。他们把分解这一庞大数字的任务分成若干个分步骤，又把它们分给许多计算者。他们总共招募了五大洲25个国家的600名志愿者。这些人通过因特网保持联系。集体劳动得出的结果p是一个64位数：

4905295108476509491478496199038981334177646384933878439
908200577

通过p除N得到q。100美元的奖金摊到600名合作者身上，每人只有17美分。

位数越多，人们分解一个大数字花费的时间急剧增加。如果从129位增加到300位，花费的运算时间要增加10万倍。这使RSA加密充满魅力。破译密码不是关键，重要的是能否“快速”破译密码。魏斯先生和施瓦茨女士通过密码商定于星期四约会，格劳先生的电脑在30年后才在屏幕上显现破译的信息，这对心怀不满的他而言已无济于事。

非对称但快速

与公开密钥的优点相对,即使利用快速的计算机也需要大量时间运算大数字,尽管人们只是在大数字 N 的余数范围内运算,所以出现的数字不可能大于 N。但是倘若密码必须安全可靠,N 必须庞大。这样,加密和脱密时出现的数字也庞大,计算也就成了一个费时的程序。但是还有一种集对称加密法的快速和非对称加密法的安全性于一身的可能性。

就对称加密而言,我们取随机数字的绦虫式密钥作为例子,就像我们在 153 页中使用的那样。为了能相互理解,发件人和收件人事先必须互通随机数发生器的基数。他们可用 RSA 加密法传送这个基数。情况如下:

施瓦茨女士在电脑内安装了 RSA 程序,并向大家通告了她的 N 和公开密钥 E。魏斯先生想给她发一封密信。他写下明文,并用字母表中的序号代替明文字母,得到数字式明文。尔后,他选择一个基数,并以此启动他的随机数发生器,以便制造一个很大的绦虫式密钥,然后如 153 页所述,把数字明文和绦虫式密钥相加得到数字式密文。这对施瓦茨女士还毫无用处。她不知道她能以此制造相同的绦虫式密钥的基数。魏斯先生此时启动他的 RSA 程序。用施瓦茨女士的 N 和公开密钥 E 加密基数。然后他先把经 RSA 加密的基数寄给她,再向她发送用对称加密法得到的数字式密文。

施瓦茨女士启用她的秘密的 D 破译基数,用此启动她的随机数发生器,得到魏斯先生使用的同样的绦虫式密钥。她

从密文中减去绦虫式密钥得到数字式明文，轻松地把它转换为字母式明文。在此过程中根本没有交换秘密的密钥数字D，而且对称加密法中的密钥——基数也只是在加密后被传送的。

魏斯先生可以替每份消息选择一个新基数。传送分两步进行。他用施瓦茨女士的公开数字N和E加密基数，又用它组成自己的密钥字，并把将到的数字置于要传送的文本的开头。它可能是给施瓦茨女士的消息的前10个符号。尔后，他让利用绦虫式密钥加密的数字式密文紧随其后。施瓦茨女士用自己秘密的D破译密文信息的前10个符号得到基数，用这基数让她的随机数发生器制造出绦虫式密钥。她从密文中减去绦虫式密钥得到数字式明文，从中她能取得字母式的明文。

今天在实际操作中正是用了这样的方法。密码程序PGP(《绝对隐私》，见附录D)用RSA传送密钥，但却用对称法加密。

世界银行利用一种名为SWIFT的加密方法保持联络。SWIFT是世界银行电信协会的缩写。在此也使用RSA传送对称法的密钥。对真正信息的加密则以传送的密钥在DES程序中产生。

至此，我们让魏斯先生用N和公开密钥E，施瓦茨女士用N和秘密的D加密。E和D实际上是完全等值的。用E加密的电报只能用D脱密，反之亦然。施瓦茨女士不仅能用她的秘密的D(和她公开的N)破译详细的信息，而且也能把用D加密的信息发往世界各地。不仅是魏斯先生，每个人都能用众所周知的公开密钥E(和N)对它进行脱密。这有何益处？能用施瓦茨女士的公开的E脱密的信息一定是用她的

秘密的D加密的。由于只有她知道秘密的D,因此,能用E脱密的密文一定是从她那儿发出的。这就如同她亲自签名一样保险。

13

芯片，不可逆函数和捕鼠器

无论谁将某地城市储蓄银行的因特网调出，都会进入一家虚拟的银行分行。顾客可以在那里的假想柜台前存款、取款或办理有价证券业务……于是存取单据以光速进入到银行的计算机中，不过后来的手续是用手工操作的。

克里斯托夫·泽格[①]

小时候我们听过格林兄弟写的《狼与七只小山羊》的悲惨故事。我一直在想这则故事里为什么没有提到过羊爸爸。他是不是因为另有新欢而遗弃羊妈妈和她的7个小宝宝？不管怎样，当可恶的老狼一边用裹着软面团的爪子敲着大门，一边嘴含浆糊、尖着嗓子轻声喊道："'亲爱的孩子们，让我进去吧，我是你们的妈妈，我给你们每个人都带了些礼物呢'时，故

① 《经济周报》，48，1996年11月21日，第194页。

事情节达到了高潮。7只小羊看到脚爪,同他们瞧见的一样,爪子是雪白的,而且,小羊听见狼说话的声音如此轻柔,他们就相信那的确是妈妈,于是打开门让狼进来。"

大家都知道,接下来会发生什么事情。如果羊妈妈不仅叮嘱她的孩子们提防粗暴的声音和黑爪子,而且还告诉他们一个明确的辨别暗号,那么,这个故事也许就不是这种结局。

老羊和小羊最好能读书写字。羊妈妈便可以这样吩咐:"我回来时从门缝里塞进一张纸条,上面有我的签名,凭这个你们就可以分清门外站的是不是你们的妈妈。"这样,小羊就能依靠这张纸条。这犹如在某些情况下,只有当专家将签名与别的笔迹相比较鉴定为真迹后,我们,甚至法庭也一样,才能相信某一带签名的文件的真实性。

羊妈妈也可以跟小羊们说定,塞进门缝的是一块带字母图案的手帕,这也可以作为识别暗号,因为那只恶狼一时很难弄到相同的手帕。

当然她也可以和孩子们约定一个口令,一个恶狼不知道的数字组合,如那位不知去向的孩子们的父亲的生日。

今天,我们也许会说这一家应该安上一把电子门锁,每个想进入这座房子的人都必须输入一组特定的数字。许多国家都有这种安全系统,特别是在巴黎,我在那儿经常看见这种门锁。只有拿到密码的人才可将门打开。如果恶狼对密钥一无所知,哪怕那只是一个3位数,它或许也得尝试上百次,才能发现这组排列正确的数字。

这样,我们就有3种让别人识别自己的方法。羊妈妈可以通过她的"身体",如她的爪子,或者通过对某样东西的"所有权",如一条带字母图案的手帕,或者通过她的"知识",如一

个口令，来证明自己的身份，也就是说，这取决于她有些什么外貌特征，她拥有什么物件，以及她知道些什么。

我是谁

日常生活中我们不时地需要证明自己的身份。当检查身份时，只要相貌得到熟人的确认或者出示不易伪造的附有照片的证件就可以。银行的自动取款机在打印我账户上的最后一笔交易时要求我出示取款卡，只要它没有落入他人之手，我敢肯定，别人是无法看到我户头上的拮据状况的。但在支付现金的自动取款机上只塞入取款卡是不够的，我还必须输入我的密码，让自动取款机确认，这张取款卡的确是由我塞进去的。

当我想在哥廷根计算中心使用电脑时，屏幕上首先就会问我究竟是谁。输入我名字的简写后，电脑才能确认我是否有资格分享这个计算中心的成果。然而，由于每个人都有可能输入我名字的缩写，所以现在电脑还要求我输入“密码”[①]，这就是所谓的我的密钥，是几年前我申请使用电脑时，该中心分配给我的。密码是一组字符，大概是 g7"kky = 7。如果我想避免别人以我的名义溜进该中心计算机系统，就必须对此保密。别人一般不可能猜出这个密码然后干出不法勾当。

我的密码由 8 个符号组成，它们中的每一个都可以是字母，数字或者 $ ，& 或 = 等等特殊符号，共有上万亿种可能性。即使某个窃码者企图将所有可能性试遍，他在有生之年也不

① 在计算机德语中引进了英语词“password”（密码），代替德语词“Kennword”或“Losungswort”。

可能通过这种尝试发现我的密码。在计算中心,一旦该密码被分配给我之后,就再也不会在别处出现。后面我们会谈到电脑是怎样通过它识别我的,密码展示的是一种通过知识鉴别身份的方法。只有我知道这一密码,当我将其输入电脑时,电脑就知道,那的确是我。

然而,存有重要信息的电脑就如一栋一般人不能进入的楼房一样,必须更好地防范非法入侵者,而不只是通过塑料取款卡、带照片的证件或密码。例如监狱或防止商业间谍的实验室就属于这种情况。另外,它也很适合中间站,在那里按照销毁核武器框架协议堆放着闲置的钚。

这样一来,身体特征也被纳入电子识别方法。一个人最可靠的标志是视网膜上小血管的结构。有专门的仪器通过红外线照射人的眼睛,相连的计算机将记录下的视网膜结构与储存中允许人内的人的视网膜结构进行比较。如果它不与任何储存中的结构相符,那么该被检查者就不允许靠近钚。

就可靠性而言,视网膜法比指纹法更先进。指纹法是将被检查人的手指头放在一块玻璃板上,皮肤的纹路图将与电脑中贮存的指纹进行比较。较先进的仪器还须测量手指的脉搏,电脑据此可以判断它前面放着的是一个活人的手指,而非电脑黑客把他的爱好玩得太过火。指纹法在使用时没有视网膜法安全可靠。如果被检查人手指某处被灼烧,电脑有可能就无法再将它识别出来。

羊妈妈已采用过的声音比较方法在今天的刑事侦察技术中得到广泛应用。所以勒索犯一接电话就会被该方法识别出来。每个人都可以让电脑识别自己的声音,电脑会建立一种声音模式并把它与已贮存的允许入内的人的模式相比较。但这种方法容易出错。当楼房上空有飞机飞过时,一旦说话人

得了感冒、咽炎或使用麦克风，电脑都有可能无法再将其辨别出来。

每一位电报员用莫尔斯电码发报时都有自己的“手迹”，他敲字母 D(长、短、短)或字母 U(短、短、长)的节奏以及与下一字母的时间间隔都可标识这位坐在莫尔斯键旁的发报员。例如在两次世界大战中，这一点就显得十分重要，因为如果按键旁突然换了一位发报员，有经验的收报员通过节奏就可察觉到。某个间谍一直自由地生活在敌国并定期发送其间谍活动信息，如果他被发现，收报员也能通过这种方式发觉。敌方发报员一旦以这个被扣押的发信人的身份发送迷惑对方的虚假信息，就会由于是另外一种“手迹”而被识别出来。甚至当人们将被俘间谍“转向”并强迫他亲自发送假信息时，他也可以改变节奏，以此作为信号告诉自己人不要相信这一信息。

今天，这种特性在稍作改变后被应用到电脑识别当中来，因为不仅莫尔斯电码的键人，而且在打字机键盘上的击键节奏都是每个打字员的特征，所以一台电脑中会存入合法使用者独特的击键节奏，接受检查者必须输人一段文字，电脑会测出速度和时间间隔并同样又与贮存的模式进行比较。

同样，电脑也可采用签名处理法。由于一个人的两次签名不可能一模一样，因此，电脑需要一个能区别关键与可忽略特征的程序，一般来说起决定作用的是写字者的收笔位置和签名速度。

我们不想借助电脑将一个陌生人的账号洗劫一空，也不需要任何核材料钚。尽管这样，我们仍必须时常证明自己的身份，以此确认我们是否有资格将汽车停人公司的停车场或不用现金就能在商店购物。

塑料卡

以前我们几乎什么都用现金来支付，今天我们的钱包里装满了塑料卡。

最初的塑料卡很简单，上面是凸压号，卡号，通过它可辨别发行人和持卡者，有时还有持卡人的住址，无需任何电线联接就能用机器读出这种卡，于是它很快就风行全世界。这种类型的信用卡导致的结果是：成堆的书面证明及汇款单。因此持有这种卡以及与此相关的审定并不便宜，于是人们在这种卡上安上约12毫米宽的磁条，原来的凸压数据通常会在上面再次被磁化储存。凸压技术在欧元支票卡上已被打印技术取代。机器能够读出磁条，磁条里还能包含其他信息，如信用卡最近一次使用的时间。如果想查一下自己的账面情况，只需将卡插入银行里的识读机，阅读机读出磁条，确认该卡是否属于该银行中的一个账户，然后打印出该账户最近几次的账面变动情况。这种简单的信用卡不仅能够满足银行结单打印机的需要，而且在阅读机能够读出磁条的条件下，许多商店单凭该卡就可出售货物，当然顾客还必须签字。

如果仅涉及银行结算，对此不会产生任何异议，但用信用卡在商店购物可又是另外一码事。除商店里的读卡机能读出磁条外，原则上每个人都可将它读出，因为有测量磁条周围磁场的仪器。不法分子可将我信用卡上的这条信息转移到另外一张卡的磁条上，然后在古尔梅特饭店用我的户头美食一顿。总的来看，这种简单的磁条卡的安全性能不高。如果它在短时间内落入他人之手，或者我将它遗失了而又没及时冻结账户，那么我将很有可能观察到自己户头上的可怕动向。

因此，严格地说，我的银行不会单单只信赖磁条卡。自动取款机虽然能够辨别某卡是否能够使用某一账户，但除此之外它还想知道，操作该卡的是否为合法持卡人。为此我必须额外用知识来证明自己的身份，于是银行就分配给我一个秘密数字。

密码——简易版本

下面我将介绍顾客是如何受到保护的。我不会详细说明我们今天的银行是如何做到这一点的，而只是以一种简单的模拟向大家展示，人们原则上可以怎样利用一个密码建立一种防止不法分子支取钱款的安全系统。我可不愿把我的钱交给我的简单模拟银行保管。值得庆幸的是现实生活中的银行使用的操作方法复杂得多。

这种密码的英文名叫 Personal Identification Number（身份证号码），缩写为 PIN。自动取款机除了需要磁卡外，还等着我准确无误地输入我的 PIN。当然，如果 PIN 本来就存在磁卡上，那这一点就毫无意义。这样的话，不法分子就能复制我的卡号，利用他的非法阅读机抄下我的卡号，并以此在自动取款机前冒充我。

有一种可能性是在银行的电脑里存入所有与账号相配的 PIN（图 13.1）。如果自动取款机辨认出了我卡上的账号，那么就可以检验我输入的 PIN 是否与电脑储存的相符。如果对，则吐出钞票，不对的话它将再给我一到两次输入正确 PIN 的机会。如果我输得不对，它会发出警报或没收磁卡，无论如何也不会给出钞票，这是一种简单而又可靠的方法吗？

银行电脑储存器

账号	明文 PIN
0235283	4382
0233222	5612
0317388	6526
0285734	7514
0285247	4700
0222802	3966
0241923	7674
0244350	6286
0256552	8154
0264325	5006
.....	...
.....	...

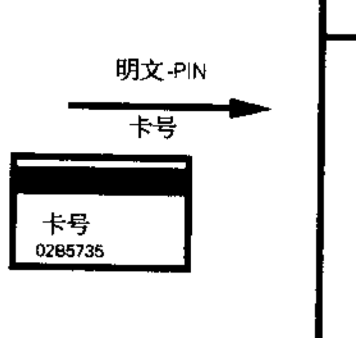


图 13.1:利用磁卡和密码进入银行的简单途径。银行电脑上储存了所有用户的卡号和密码。电脑将识读机读出的卡号以及用户输入的密码,即明文 PIN 同电脑储存的数值进行比较,如果输入的 PIN 与卡号相符,自动取款机将给出所需款额。

如果说完全安全可靠倒也不是。银行的某处储存了所有账号的 PIN,不少职员可以进入银行电脑,为数极少的人员还能进入用户的 PIN 数据库。在现实生活中的银行里这点无关紧要,因为众所周知,所有银行职员都诚实可靠。但在我的假想模拟银行里有一位职员被炒了鱿鱼,因为他在上次公司庆典上与行长夫人打情骂俏,玩得太过火。想一想,万一他还赶紧让电脑打印了一份 PIN 一览表,以便日后利用,那怎么办?

银行电脑里储存的 PIN 并不能保障用户的利益。如果这位心怀不轨的职员接触到我的卡,那他就可以凭一份复制件及我账户的 PIN 长驱直入我的户头,直至出现赤字。

我如何使密码保密?

我的支票卡有一个密码。此外我还有两张不同的信用卡,它们分别都带有一个密码。为了能在国外用信用卡给家

里打电话而无需向旅馆支付额外费用，发行信用卡的机构又分别给我设置了使用这项特殊电话服务的密码，于是总共有5个密码，我必须尽可能地在脑子里记住它们。人们再三叮嘱我不要把它们都写在一张纸上然后放入同一只钱包，我也不会这样做。但我还是记不住这些密码，于是我就以加密的形式把它们带在钱包里，甚至放在同一个格层里。

加密很简单。假设，密码为3810、5741、6739、8422和6284，现在我想出一个我必须记住的4位密钥数。我们将看到，怎样选择一个数字，能让它随时从记忆中再现。比如，我选择6921作为密钥数，然后拿出我的5个密码，分别加上密钥数，不考虑十进位：

3810	5741	6739	8422	6284
6921	6921	6921	6921	6921
9731	1662	2650	4343	2105

最底下一行中是我加了密的密码，我现在可以放心地把它们写在一张纸上带在钱包里。我甚至还可以在每个旁边标明它属于哪张卡。

减去密钥数后，我的密码又重见天日：

9731	1662	2650	4343	2105
6921	6921	6921	6921	6921
3810	5741	6739	8422	6284

我现在只需记住我的密钥数，而不再是这5个密码，但还可以简单些，我只要记住任何一个能让我想起并记住密钥数的单词就可以了。我将它写成一行字母：

R E C K L I N G H A U S E N

现在我在下面写上与这些字母相应的字母排列顺序数，即A下为1，C下为2，两个E下为3和4等等，大于9的数去掉十

位,如就用0和1代替10,11。

R E C K L I N G H A U S E N

2 3 2 8 9 7 0 5 6 1 4 3 4 1

这样,从 Recklinghausen 这个词我们得到的数字是23289705614341,它的前面4个数构成密钥数:2328,所以如果你无法记住你的密钥数,不妨记住"Recklinghausen"或者其他一个较长的单词,这样你可以随时从中重建你的密钥数。

这种方法的弊端是:万一有人知道你的某个真实密码,那他可以把它从加密的密码上减去,得到你的密钥数,从而为他打开了通往你的所有密码的大门。

密码——已加密

密码学能在这里帮上忙。银行在给我 PIN 的同时也将它加密,从我的"明文 PIN"中制造一个"密码文 PIN",我取得明文 PIN,而银行将密码文 PIN 存入电脑。

我举一个十分简单的例子,这同样不会在现代化的银行里发生,并且我还采取一种简单的加密方法:在 PIN 上加上一个密钥数。这是一种相当原始的方法,不能推荐给任何一家银行,但我们可以从中知道其原理。

银行给我明文 PIN,如 2163。银行有唯一的一个适用于任何用户,但严格保密的密钥数,我们假设这个号码为 4637,银行将它与我的 PIN 相加,不考虑十进位制:

明文 PIN	2163
密钥数	*4637*
密文 PIN	**6790**

银行在告诉我明文 PIN 后,它的电脑会自动销毁这个数字。现在银行里没人知道我的明文 PIN。那儿存入的只是我的密文 PIN。现在只有知道密钥数的人才能发现我的明文 PIN,途径是从银行储存的我的密文 PIN 中减去密钥数,同样也排除十进位制。这个密钥数必须在银行里高度保密。

现在我带上卡和分给我的明文 PIN 去自动取款机上取钱(图 13.2),我插入卡,输入明文 PIN,银行电脑将输入的 PIN 加上密数,不考虑十进位制,同上得到 6790,然后将结果与我的密文 PIN 进行比较。如两者相符,自动取款机就吐出现金。

银行电脑储存器

明文-PIN

卡号

卡号
0285735

将明文PIN换算成密文PIN

账号	密文 PIN
0235283	
0233222	
0317388	
0285734	
0285247	
0222802	
0241923	
0244350	
0256552	
0264325	
.....	
.....	

图 13.2:用保密程度较高的磁卡和明文 PIN 提款。银行电脑拥有一种将明文 PIN 转换成密文 PIN 的加密方法。发行磁卡时电脑将一个明文 PIN 告诉用户,将其编密并在自己的储存器消除该明文 PIN,这样存入的就只是每个用户的账号和密文 PIN。谁要想从自动取款机上取钱,必须插入磁卡,输入明文 PIN,电脑将其加密并将得到的密文 PIN 与存入的密文 PIN 进行比较。如账号与密文 PIN 相符,自动取款机就会吐出现金。

那位心术不正的银行职员现在就遇上难题了。虽然银行电脑存入了所有用户的密文 PIN,但不知道密钥数他是无计

可施的。当然无论如何不能让他知道这个密钥数。这个数字只能存在一个只有行长知道的地方，而且他在自己的夫人面前也不能泄露，尽管如此，某些地方还是存在着能够将所有用户的明文 PIN 都计算出来的数字。

为了避免这种情况，人们采用所谓的不可逆函数。在我们把这个问题了解清楚前，让我们还是换个话题，对数学稍作浏览。

数学上的捕鼠器

捕鼠器里放一块奶酪，老鼠很快就会跑过来，一旦它进去了就再也出不来。在 RSA 方法中，魏斯先生能轻而易举地用施瓦茨女士的公开密钥给一篇明文加密。如果他将明文遗失，就再也无法读取它。他自己加密的东西连自己也解不开。这和老鼠进了捕鼠器一样：往一个方向去很容易，往相反的方向却不可能。

因为明文和密文可以毫不费力地转换成数字，所以人们也可以这样讲：将明文数字转化成密文数字不成问题。但问题是将密文数字恢复到原来的明文数字却很困难。将一个数转化成另外一个数，其中转化朝一个方向简单易行，向相反方向却很困难的现象叫不可逆函数。这种现象出现在各种各样的场合。

如果伽利略从某个含有一项科学发现的句子中造出一个换序词[1]，这由明文到密文的过渡就是不可逆函数。人们很容易将一首诗转化成一个换序词，为此只需将字母按字母表

① 换序词就是变换顺序构成的词或短语。——译者

顺序排列即可。但尝试一下将一个换序词变成一首诗。向换序词的过渡就是一个不可逆函数。在 RSA 方法中密文是明文的不可逆函数，将两个大的素数相乘相对较简单，但实际上却不大可能将所得数分解成它的因子。这又是一个去时容易回时难的例子，我们已经知道，RSA 方法的可靠性正是建立在此基础之上。因为下面将介绍 RSA 方法的不同应用方式，故我在方框中将其再次作一扼要说明。

运用幻数 N、D 和 E 的 RSA 方法简介

1. 用幻数 N、E(或 N 和 D)将一段数字式明文 K 加密：连续排列 KXKXKXKXK……直到写完 E 次(或 D 次)K 为止。做乘法，再将乘积多次减去 N，一直减到其结果比 N 小为止。所得数字即为数字式密文 G。

2. 用 N 和 D(或 N 和 E)脱密：如 G 是由 N 和 E 加密产生的，那么按照以上规则用 N 和 E 将其再次加密。则重新得到数字式明文 K。如 G 是由 N 和 D 加密产生的，那么用 N 和 E 将其再次加密。

3. RSA 的不可逆函数：用 N 和 E 将数字 K 变成密数 G，于是手中没有 D 的人绝不可能从 G 还原 K。

不可逆函数对什么有利？如果魏斯先生无法读出自己加密的信件，这与我有什么关系？然而，如果除我之外还有其他人知道我用于从自动取款机上取钱的密码，那这与我的关系就大了。而且不仅是不想让别人知道，我也不想让银行知道这一密码。在我被告知这一密码之后，银行的电脑应该将它删除，不过我希望银行的自动取款机能通过它认出我来，而且实际上这一切都是可能的，因为不可逆函数的存在。不过我们先得经过好些阶段才能达到这一目标。

不可逆函数保护我的银行账户

刚才我让银行采用一种十分简单的方法对我的 PIN 加密。正如我们在第十二章中看到的一样,银行除此之外还可以采用一种 RSA 方法将我的明文 PIN 加密。

我们还记得:RSA 方法中有三个幻数,一个大的(N)和两个小的(E 和 D)。用 N 和 E 加密过的,不能再用 N 和 E 脱密。到目前为止我们仅将 RSA 法应用于需加密并被收件人脱密的信息上。现在我们只想将它"半"使用,即只加密而无意脱密。借助密钥 N 和 E 我们将一个明文数转化成一个密文数。这种转化是一个不可逆函数——这对我们已足够了。所以接下来我们不再谈到密钥 D。

银行掌握了 N 和 E,用这两个数字将我的明文 PIN 加密得到我的密文 PIN 并将其保存。银行在告诉我明文 PIN 后随即在电脑中删除这一数字。于是现在全世界除我之外无人知道我的明文 PIN。银行职员最多能发现我的密文 PIN,而这对他毫无用处,因为从密文 PIN 到明文 PIN 的途径被隔断了。这正好就是不可逆函数的意义所在。

现在谈谈我自己。当我告诉自动取款机我的明文 PIN 后,取款机用银行的不可逆函数计算出我的密文 PIN 并将其与储存在电脑中的密文 PIN 进行比较。如两者相符,取款机就会给出现金——当然也立即从我的账户上划扣这笔钱。

这种方法真的完美无缺吗?在我简化了的模拟银行里安全专家们大概一点也不满意这种操作方法。因为从取款机键盘到银行电脑之间存在一条电线。只要有人在这条电线上搭线,就可以知道我的明文 PIN。这并非难事。我的 PIN 通过

电线时带有的电子脉冲波会产生电磁波，类似于无线电波。这条连接电线就充当了天线的角色，向各个方向发射电磁波。所发射的电磁波几百米之外都可接收到。借助一台合适的接收器，人人都可以窃取我的明文 PIN。只要谁手里有我的支票卡，就能从任何取款机上从我的账户上取款。如果明文 PIN 经过电线时是以加密的方式传递的，那么简单磁卡的这一缺陷就会被克服。实际生活中的银行就是如此操作的，不过不久人们还将另辟蹊径。

磁卡上的磁条由氧化铁制成。有人曾经戏称：正因为磁卡是由氧化铁做的，其聪明程度与氧化铁差不多。

支票卡中的电脑

当我在 50 年代中期第一次有机会使用电子计算机时，这种仪器占据了一整间房子。数据被存在一只带有磁层的大卷筒上。读、写磁头不停地接触转动的卷筒。我们今天的电话卡上装有电脑，它们的储存量比电脑石器时代那台恐龙般的电脑上卷筒的储存量还大好几倍。今天称为芯片的微小物体，其整个在卡上只占据不到 20 平方毫米的面积。这种芯片不能再大，否则卡片被弯曲时它就会折断。从外面看上去有许多彼此分开的金黄色小金属片，即触点。它们是计算机与外界的连接。就是通过这些触点计算机从自动取款机上接触趋动电源，就是通过这些触点计算机从自动取款机上接收数据；就是通过这些触点计算机将数据输送给自动取款机。在卡片材料上有一处凹陷，里面有一层金属面，真正的电脑芯片就位于金属面以下的中间位置。把磁卡插入自动电话机后，触点将卡与电源连接起来。我们银行的支票卡目前只有这种

简单的磁条，不过不久将用上这种微型芯片。这种卡的储存器可读可写。磁条将由带电荷的微电容器取代，它将把以双位数的形式输入的数据记录下来。一个充电的电容器为 1，没充电的电容器为 0。一系列微型电容器可以将卡号、银行及持卡人名称等数据以双位制形式的数字储存起来。即使过了若干年后被分配的电荷也不会丢失。电脑可以改变其电荷状况，存入的数字也可用新的替换。而且芯片卡上的电脑不仅能够储存，而且还能计算。

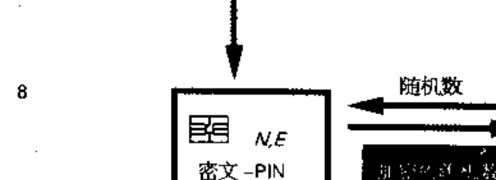
我的简单模拟银行中的操作程序大约是这样的：银行将带芯片的支票卡签发给我的同时，也将我的 PIN 告诉我。银行用不可逆函数给我的 PIN 加密，我们假设用 RSA 加密法，按照 RSA 方法所要求的取一个数字 N，N 必须是两个相当大的素数的乘积。在我的模拟银行中，这个 N 对每一个用户而言都是相同的，不过银行会为每位用户算出一个独自的密钥数 E，正如我们在附录 C 中为确立三个幻数所做的一样。所以银行也为我准备了一个数字 E，这就是我的密钥数，银行电脑用它来给我的明文 PIN 加密，得到我的密文 PIN。电脑将这个 N，我的密文 PIN 和我的 E 写入我卡中的储存器，随后在银行里，我的明文 PIN 和密文 PIN 被删除，银行在储存器中只保留我的密钥数 E。

我现在走到自动取款机旁，将卡插入插卡口并输入我的明文 PIN，于是卡上的芯片开始进行加密。它现在已接通电源并开始工作，按照 RSA 方法，它用对所有用户统一的“N”和我个人所有的“E”给我的明文 PIN 加密，然后将结果与储存在电脑中的我的密文 PIN 进行比较（图 13.3）。如这两个数相符，我就完成了第一步。现在已确认，我是该卡的合法持卡人。

2

4

8





银行电脑的储存器

账号	*E*
0235283	*540254482*
0233222	*493716048*
0317388	*601825925*
0285734	*615948260*
0285247	*604826048*
0222802	*259269369*
0241923	*371604937*
0244350	*159370482*
0256552	*592693692*
0264325	*581369247*
.....	.....
.....	.....

图 13.3:用芯片卡在自动取款机上取款。银行在签发这种卡时会在用户的芯片卡上写出密钥数 N 和 E,可以用它们按照 RSA 方法加密。银行还配给用户一个明文 PIN,并用 N 和 E 为其加密,这样,银行就得到用户的一个密文 PIN,同时把它写在他的卡上,但又会在银行的储存器上删除。所以银行电脑中储存的只是每位用户的账号和各自的密钥 E。

现在,用户走到银行自动取款机跟前,插入他的芯片卡并输入明文 PIN。卡上的芯片用 N 和 E 给明文加密并得到这位用户的密文 PIN,然后将它与银行存入储存器中的密文 PIN 进行比较。如两者相符,则确认该卡与用户相符。于是银行电脑中的一台随机发生器开始运作。它为卡上的芯片提供一个随机数字。用 N 和 E 为其加密并把它交还给银行电脑,而电脑在此期间也同样用 N 和用户的密钥数 E 给这个数字加了密,于是现在可以进行比较了。如果芯片和银行电脑在为随机数字加密时得出同一结果,那么自动取款机就可以毫无阻碍地支付现金。

接下来的问题是：我的卡为我打开了通往银行账户的合法通道吗？现在由银行电脑对我的卡进行检验。像一场考试一样，电脑向我的卡提问，卡必须正确回答。银行电脑会给卡一个随机数字，于是我的芯片用 N 和我的密钥数 E 给这个数加密，并将结果，即被加密的随机数字交还给电脑。在此同时电脑也用 N 和它知道的我的密钥数字 E 给这个随机数字加密，然后检验我的卡是否也得出了同样的结果。如果答案肯定，那它就知道，该卡允许进入我的账户。

让我们再总结一下：我自己知道我的明文 PIN，而我的卡相反只知道众所周知的 N，我的用 N 和 E 加密的密文 PIN 和我的密钥数 E。我们来看一看，现在有一个银行职员搞到一张被储存的密钥数 E 的清单，但他不能制作我的卡的副本。他不知道我的明文 PIN，而我的密文 PIN 也没有储存在银行里。此外取钱时，我的明文 PIN 不会在我和银行电脑之间传递。当然，取款机不能被人操纵，而且在我输入 PIN 时，它不能将 PIN 既送到我的芯片上又送到另一台个人电脑上去。这样一来，在我与银行计算机中间通过电线传递的到底是什么呢？仅仅只是新的随机数字及其加密过程而已。

塑料卡上的钱夹

银行职员迈尔热爱自己的工作，银行里的这份工作真是丰富多彩，时下尤其如此。一位顾客坐到他的对面，显然他想注销他的账户，因为他打算取走所有金额，几乎有近 10 万马克。在后室里，这位顾客当着迈尔的面清点一张张小面额钞票。这位顾客随后会将钱往衣兜里一塞，还是放入塑料袋中扛走呢？他并没有随身携带公文箱。数钱的时候，迈尔发现

这位顾客的面部表情由最初的几分阴沉显然地明朗起来。当最后一张 10 元钞票放到桌面上时，来访者突然容光焕发。“我实在太高兴了”，他说道。“现在您又可以把这些钱存回我的账户上去，我只是想看看，是否它们都还在那儿。”

顾客存入银行的钞票，无论现在它在何处，反正早已不在银行那儿了。我们已习惯不用现金支付，我们既不把钱换成纸币，也不把硬币放在长统袜中。只要我们在法律允许的范围内活动，我们就不必将钱放入公文箱，带着它穿越边境，我们可以将我们银行里的钱汇到世界的任一角落，无论是火奴鲁鲁还是悉尼。如果我向香港的孔福先生汇一笔超过一万马克的款项，我的银行不会将一个装满钞票的包裹寄到那儿，因为实际上我在银行里没有一分钱。只是在一个本子或一台电脑上明确地记录着它欠我多少钱。我的汇款实质是我的银行通知香港的银行：“请向用户孔福支付价值一万马克的港币，为此我方欠您这个金额。”当然，我的银行同时会将这一万马克记入我账户的借方账下。

在不用现金流通的同时，我们却仍用现金支付账单。大家把钱放进皮夹里随身带着，因为我们既不通过汇款也不用信用卡买电影票或乘公共汽车。现金交易依然在日常生活中占主导地位。此外现金还是匿名的，从一张纸币上无法看出在我之前谁曾使用过它。这种匿名性保护了我的个人生活。

借助密码处理方法使随身携带电子千元大钞成为可能。如我在银行里的账面情况一样，这种钞票现在只是芯片上的一个数字。要想让这种电子货币真正流通起来，必须让用户感到尽可能的简捷方便。银行用户按照银行的要求得到一张加载的钱卡，也就是说，这张卡上存入了一笔特定的款额，像一张崭新的电话卡上满是一个个钱的单位一样。用户拿着这

张卡去商场购物并在付款时将卡插入那儿的阅读机，商品的价格会自动从存在卡上的总额中减去，而商场又是与银行有联系的，银行随后会将相应的金额记入商场账户的贷方下面。一旦卡上存入的钱被用完，用户必须到银行给卡“加油”，费用当然算在他的账户上。

为了使读者弄懂这种方法原则上是如何运作的，我将以我的假想模拟银行为例，对芯片卡上的电脑、商店里的解读机以及银行里计算机上的计算过程作一说明。以前我到银行的窗口取现金，而现在是银行在卡上写下一个数字，这即是我的电子现金，同千元大钞一样。如果我想用它购物，就把这个数字交给商店老板，他必须检验，看他得到的这个数是否真正合这么多钱。如果他把这个数目交给银行，那么这 1000 马克的款项则会被记入他户头的贷方下。

这是怎么运作的呢？其实存在着无穷多的数字。要是数字能当作货币使用，那么人人都能随心所欲地拥有大笔钱财。采用纸币的时候，一定也曾产生过类似的争论。假如纸可以当作钱，那人人都将富有，因为到处都有大量纸张。我们知道，不是每张废纸都有钱的价值，只有那种赋予了特殊性能的纸张，比如带有防伪印刷，才有货币的价值。这一点与用于付款的电子货币是同样道理。只有预先设计过的数字才能防伪并能代替货币使用。

让我们在一个简单的模型中来看这一点。图 13.4 对此进行了图解分析。银行采用一种 RSA 方法。它拥有 3 个幻数，N、E 和 D，它用 N 和 D 加密的东西就只能用 N 和 E 来脱密。现在我想从我的银行获取一张 1000 马克的电子货币。第一步，银行会从我的户头上清除 1000 马克，然后任意给我选择一个数字，如 1997，实际上它会选取一个大得多的数字，

一个10位、20位或者更大的数字。它将这个数字前后写两遍，然后得到一个新的数字，在我的例子中是19971997。然后用它的密数D给这个重叠数字加密。我们假设结果为59274100698，这是我的千元电子货币。银行电脑将它写入我钱卡的储存器中。

这个数字是防伪的。无论我向哪家商店老板出示该卡结账，他们都可以完全信赖它。我去电子商品经销商那儿买了台价格正好为1000马克的电视机。付款时，我将卡插入付款处的解读机，解读机在我的卡上找出数字59274100698，就是我从银行得到的那个数字。我们记得：这个数字是银行用N和密钥D将一个重叠数字加密后产生的。现在这家商店的解读机又用N和银行的公开密钥E给这个数字脱密。它应该重新得到我的重叠数字19971997，如果结果由两个前后相邻排列的相同数字组成，阅读机将在卡上消掉这1000马克电子货币。于是我可以带着那台电视机离开商店，因为老板现在知道，我的电子货币是“真的”。如果我卡上的储存器中是任意一个无中生有的数字，那么脱密时就不会产生一个重叠数字。

现在，商店老板将我的1000元电子货币，即数字59274100698，交给银行。银行也想知道这钱是否是真的，同商店老板一样，它也检验用E脱密时是否会产生一个重叠数。如果是，银行就会把这1000马克记入商店老板户头的贷方。现在一切都有条有理——我得到了电视机，我的账户减少了1000马克，而店老板的户头上增加了1000马克。

不过银行还得确保商店老板不会多次用我的数字要求收款。为此，银行持有一份已付款项清单，即相应的数字清单。这样，兑付的时候，银行就会查看是否该数字已被使用过。

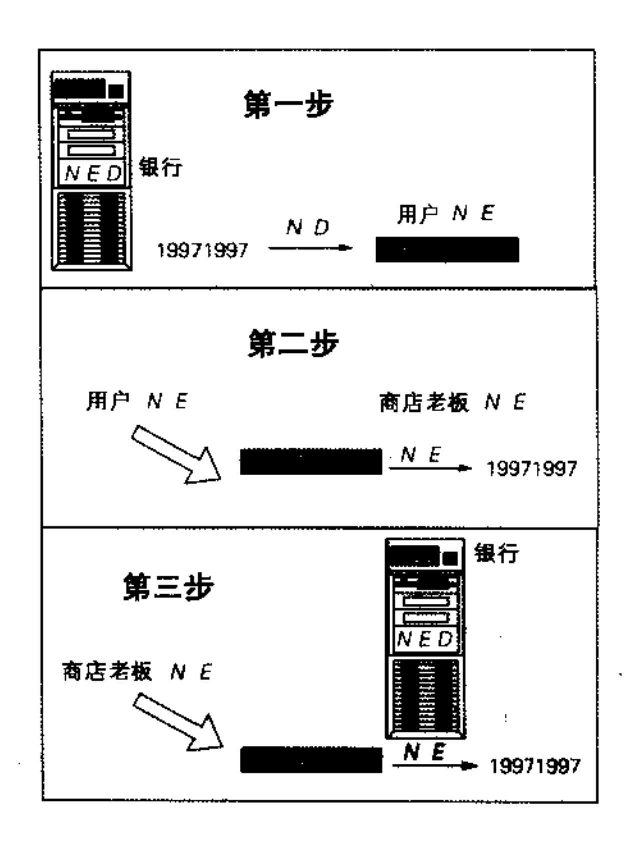


图 13.4:价值为 1000 马克的电子货币简介。银行掌握着 3 个密钥:千元钞票的两个公开密钥,大密钥 N 和另一个密钥 E;还有非公开密钥 D。
第一步:银行创造一个防伪数字。它由两个相同的数依次组成。我们称之为"双数",例如 19971997。用银行密钥 N 和非公开密钥 D 给它加密。得到的结果是 59274100698。银行在发行的千元电子货币单上记下这个数字,从顾客的账户中注销 1000 马克,并把这个数字交给他。这就是千元电子钞票。
第二步:顾客拿着千元电子货币去商场。他的阅读器用 N 和 E 对此脱密,以验证他收到的数字是否确定是一张 1000 马克。如果阅读器得到一个双数,它就知道,这货币是真的,便除去顾客金卡上的数字。此时,这个数字被储存在商店的解读器内。货币转账结束,商店能把物品交给顾客了。
第三步:商店携带这张电子货币去银行。银行首先用 N 和 E 脱密以验证货币的真实性,查看清单看它是否已被兑现。尔后替商店把 1000 马克记入贷方,并在已发行但未兑付的电子货币清单中划出这个双数。

但亲爱的银行用户们,您在实际当中不会察觉到任何这些计算过程,因为在那儿,这一切又是另一番情形,您只会发现:1000 马克不见了。

我已将这种方法简单地描述了一番。我以一张正好存有1000 马克的钱卡为例,并对如何用这笔整数付账作了说明。实际上,人们是在许多细小的步骤中将电子卡花空的,如购物,加油等等,在我们的模型中,银行还知道,兑出的 1000 马克已经支付给我,因为这个重叠数字是专门为我制作的,所以与 1000 元纸币不同的是,刚才分析的这种方法不能保障我的匿名性。我只是在此把基本过程勾画了一下,不想对其余有所改进之处深入赘述。我只想演示人们原则上能够如何从账户上将电子货币安全地带入流通领域。

今天,电子钱夹大行其道。银行和储蓄所发行一种带芯片的卡(图 13.5),上面储有 400 马克的启动资金。

顾客在商店里付款时,把卡插入解读器,解读器拭去卡上相应的金额并替店主记入贷方 1000 马克。顾客不需要密码,也不必签字。店主不必先去银行查问顾客是否透支,因为银行已在金卡的支出项目中取走 400 马克。金卡如同现金一样使用方便。顾客如果不慎遗失金卡,就好比丢了现金,谁发现金卡,就如同找到现金。

“就这么简单”,我在德意志银行的一份广告中读到,“请填您的德意志银行金卡:在终端设备或标有 Geldkarte(金卡)字样的自动取款机处,首先输入您的金卡。尔后得到您电子钱夹内的剩余额,它显示您至多可取的金额。输入您想取的金额和密码(与 EC 卡和客户卡的密码一致)。取款额自动从您的私人账户上注销。”在银行交易中,人们必须始终关注手续费。对此我又读到:“在德意志银行的机器内取钱是免费

的，原则上使用其他的机器则收取 2 马克的手续费。"

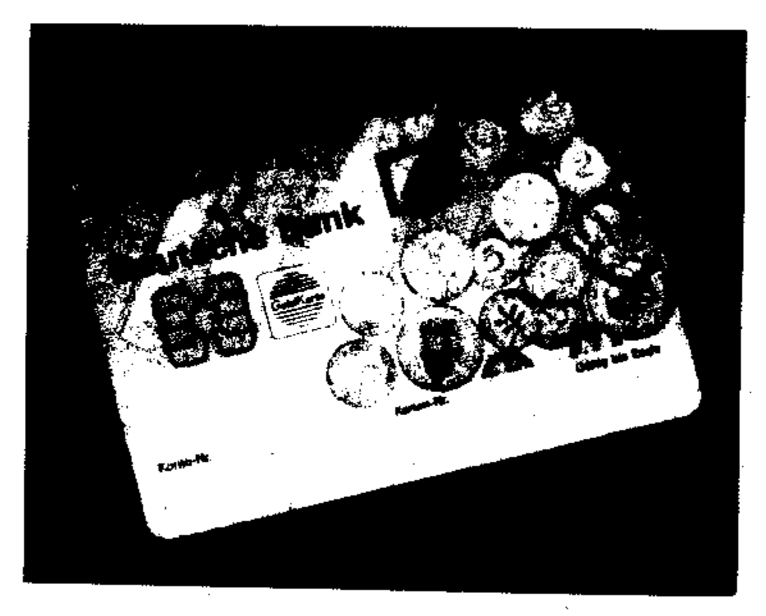


图 13.5:德意志银行的一种金卡

使用带有新型电脑芯片的电子钱夹以及支票和信用卡真的安全可靠吗？或许有人能够用我的钱生活得逍遥自在？如同保险箱窃贼们碰到每台新设计的银箱时都寻觅方法，如何智胜这个所谓可靠的系统一样，为攫取他人的金钱，电子银箱窃贼们无时无刻不在研究破译金卡芯片的秘密。我们从媒体中一再听到这样的消息，因为我们的金钱处在危险中的这类新闻的价值远远超出那些安慰性的保证，说我们的电子货币受到很好的保护。

毋庸置疑——和电子钞票打交道让我们面对新问题。计算机得花费时间计算密钥数字。世界上的大型信用卡公司总共发行了八亿张卡。今天的一部机器每一秒半就能制造出一

张卡。如果每两年更新一次卡，必须得有20台机器昼夜不停地运转。如果信用卡被换用RSA程序，以及为制造密钥数字N，那样使用155位的素数，也许得有200台机器长期制造密钥数字和信用卡。因此向分布在全球更多的顾客分派这同一种密钥，此事让人举棋不定[1] ——一个令人不安的念头。

当今时代，电子钱夹发展迅猛。至1997年末，据说在德国已发行了6000万张带有芯片的EC卡和银行卡，并已建立约10万个取款点。[2] 联邦共和国的公民们可能要拿着电子钱夹无可奈何地站在解读器面前。除了德意志信贷机构发行的“金卡”外，德国电信，联邦铁道和德国交通公司联盟计划联手发行一种“付账卡”，它能够在磁卡电话机上刷卡(用两个电话单位的费用)。另外还有“P-卡”的加盟，它由电子银行系统推向市场。哪些卡被哪些解读器解读，以及人们是否能够用金卡打电话，我们将拭目以待。目前在比利时和奥地利还不能使用德国卡。

未来将表明顾客是否愿意接受塑料钱包。

电子签名

签名的文件具有法律效力。虽然有一些尽管已签名，但在一定期限内还可收回的协议，但就一般而言，签名者本人必须承诺自己曾签名确认的文件。例如在购买地产的重大事件中，法律要求有公证人在场。他监督确系本人签上自己的名字。尔后，他也必须在文件的某个地方签名。即使签名人已

---

① 《新科学家》，1996年10月12日，第21页。

② 《经济周刊》，第48期，1996年11月21日，第188页及以下几页。

不在人世，只要一切合法，签名依然有效。如果有疑问，鉴定人可通过和其他文件相比较确认签名是否属实。

署名的弊病在于必须有原件以辨认其真伪。任何人都能廉价地进行复印，把另一份文件上的签名复制到这份上。如果用电脑发传真，这根本不费力气，可以把一份文件签名扫描进电脑内，安插在另一份文件上。也许只有专业人员才能辨清传真是否已被作弊。签名是真的，它只是在一份假文件下。因此文本经电报或传真机通过电路传播到世界各地，但收件人并不能确认这电子传送的署名的真实性。密码学能帮助解决这一难题。

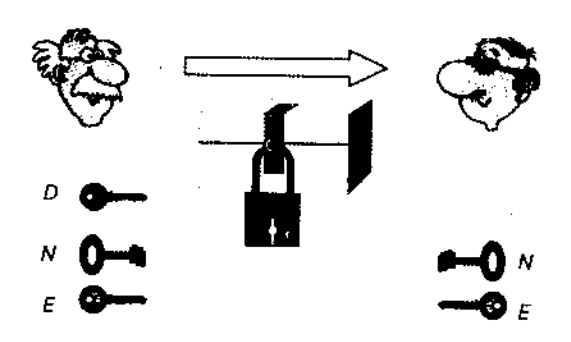


图 13.6:列举双重锁箱子一例阐述电子署名。阿尔特先生使用机器给公证人迈尔霍费尔先生写了一封信，但没有亲笔签名。尔后，他把信放入箱内并用大钥匙和秘密钥匙 D 上锁。收件人利用阿尔特先生的公共钥匙 N 和 E 打开锁。因为用 N 和 D 上锁的箱子只能用 N 和 E 开启，迈尔霍费尔先生知道这消息只能从阿尔特先生处发出。这很保险，好比阿尔特先生亲笔签了名。

图 13.6 又一次利用双重锁箱子的图解阐述了这一原理。阿尔特先生拥有 N、E 和 D 3 把钥匙。由于 N 和 E 是公共钥匙，所以收件人也有。收到箱子时，他能断定是阿尔特先生，

而非他人把信投人箱内,因为这把锁只能用阿尔特先生的钥匙 E 打开。现在转入更为实际的情形中。

阿尔特先生在泰国度假。某天晚上,他的律师和公证人,慕尼黑的迈尔霍费尔先生给他打电话,提醒他为购买出租公寓所接受的贷款的固定利息的支付期限几天后将结束。如果他不立即在一份新的贷款合同上签字,那么得马上支付 15 万马克。他因此通过传真给阿尔特先生发了一份新的贷款合同。虽然他有权替代阿尔特先生签字,但他很想在 24 小时之内征得阿尔特先生的同意。尔后,他才能替自己的当事人在合同书上签字。阿尔特先生此时想给他的律师开绿灯。但是他的律师也想确认这是阿尔特先生授予的全权,而不是某个干涉阿尔特先生业务的格劳先生。阿尔特先生有一个 RSA - 密码以应付这样的情形。公证人当然知道公开密钥是 N 和 E,但是只有阿尔特先生知晓密钥 D,他着手写下如下的字:

hierm itbea uffra geich herrn drmayerhof erwoh nhaft inmue
nchen unger erstr assef uermi chein endar lehen svert rague
berdm hunde rtfue nfzig tause udabz uschl iesse nleop oldal
txxxx

这段文字对迈尔霍费尔先生而言当然仍无济于事,因为他无法从电报中得悉署名是否真实,以及它是否确由阿尔特先生发出的。如果阿尔特先生在暹罗湾游泳时遇上一条鲨鱼不幸罹难,他的继承人可能会指控公证人没有得到全权就自行签署了一份合同,因为电报签名毫无价值可言。阿尔特先生因此用 N 和密钥数 D 加密整段文字并把结果寄给迈尔霍费尔博士。由此达到了什么目的?

我们注意:密钥 E 和 D 具有同等价值。一般情况下,用 N 和 E 加密,用 N 和 D 脱密。反之亦然。任何人都能利用阿尔

特先生的 N 和公开密钥 E 破译用 N 和密钥 D 加密的消息,当然也包括这位公证人。这并不是保守秘密,而是检验署名的真实性。如果脱密时出现一段有意义的文字,公证人就知道,这个电报必定来自阿尔特先生处,因为用 N 和 E 能脱密的密文只能由 N 和 D 加密而成。除阿尔特先生之外,没人拥有 D,其中也包括格劳先生。他因此无法将明文转换为用 N 和 E 脱密时展示出一段有意义的文字的密文。

人们可以这样用电子 RSA 密码传送文件的方法,使收件人确信文件由何人所发——如此有把握,就如同发件人在文件下亲自签上了名一样。

几年来,在银行业,特别在大公司往来文件中一直使用电子签名。这儿的各家银行和公司已按条约的形式商定承认电子签名的有效性。

电子身份证

公证人迈尔霍费尔可能对这个电子签名感到满意。他同阿尔特先生认识多年,密钥数字 N 和 E 是阿尔特本人通知他的。但即使是我们的亲笔签名,对于公证人来说,是不够的。如果您要买或卖一幢产权房,而他又不认识你本人,那他就会要求看你的护照或身份证。这类证件可以证实,的确是你。公证人得到保证,是正确的人签了正确的名字。那么电子签名是怎样达到这种安全性的呢?

整个过程同身份证颇为相同。身份证由一个机构签发。此前必须进行确认的是,你就是证件申请人,你已登记住址,递交的证件照片是你本人的照片。这个机构在你的证件上证实这些。负责签发电子身份证也必须建立一个机构,一个证

书部门。

现在我们再演示一下，身在泰国的阿尔特先生如何与慕尼黑的公证人迈尔霍费尔博士互通信息：两人从未见过面，但阿尔特先生通过朋友介绍，有意聘迈尔霍费尔先生为自己工作，而且即刻需要。为此，迈尔霍费尔博士必须得到阿尔特先生的全权委托。此前阿尔特先生已在证书部门申请了签名密码证书。他去了那个机构，证明自己的身份，并通知他们自己的 RSA 值为 N 和 E。发证处验证，阿尔特先生是否真是证书申请人，并确认，阿尔特先生是阿尔特先生，他已具有官方密钥 E，他的加密方式为 RSA 程序，并以数字 N 为基础。现在这就是阿尔特先生的身份证了。发证处可以将其打印出来，通过传真或电报发送。不过身份证暂时还没有很大意义。因为这样的证明也可由格劳先生完成，冒充阿尔特先生。公证人必须确定，身份证的确经发证处签发。

我们已知道如何设法做成此事。发证处必须在证书上进行电子签名。对此公证处自己有一套 RSA 程序。它的 N 的官方密钥 E 是大家都知道的。发证处用自己的密钥为所有签发的身份证加密。阿尔特先生现在通过电报或互联网向公证人发送一个以他的密钥加密的消息以及他的电子身份证。公证人先要借助公证处的公开密钥，为身份证脱密。如果如愿以偿，说明身份证是真的，同时他也得到了阿尔特先生的公开密钥。他可以用这个公开密钥破译密信，然后他确信，这封信来自阿尔特先生。

在这个例子中，我已经有点心急地走到了现实的前面。1996 年 8 月 12 日，德国出台了关于承认电子签名的法律草案。其中有对证书部门职责的阐释。这份草案有待于 1997 年最后公布。不过我们的银行早已在国际支付往来中，采用

相似的方式来相互签证。他们的证书部门 SWIFT(见 266 页)位于比利时。

这项数学理论作为纯数学的分支不久前还被认为毫无实际用途,而只对研究者有吸引力,这已得到改变。我们正向信息社会挺进,全球范围内的信息交流变得越来越重要。今天,RSA 程序已经可以帮助保护我们的钱财。通过它,加密的签名可以在世界各地的法庭上迅速得到确认。而这一切都建立在那些无法分解为因子的大数值上。

至今无人能分解的最小数字有 140 个小数位。在美国推行 RSA 程序的公司,每年会投 7000 美元到一个奖金罐中,每一位为当时尚未被分解的最小值找到因子的人,都会从这笔钱中获得酬金。从上次颁发奖金以来,罐中已积存了 17000 美元,且逐年递增。下一位获奖者可以得到罐中存有的总金额的 4/7,然后奖金陆续逐年存积,直至新的获奖者出现。

不过,世界各地的科学家孜孜以求因子分解大数值的方法,并不仅是为了奖金。椭圆曲线法问世已十余年,对于那些所含因子不是很大的大数,它卓有成效。采用这种方法得到的最大因子,是一个 47 位的素数。暂时还不算多。数学家们已发明了另一种方法,称为“正方筛”,同 257 页上介绍的厄拉多塞筛法颇为相似,1996 年 4 月,人们运用这种方法,成功地分解了一个 130 位的数字。

但是,依赖 RSA 程序的人从另一个完全不同的方面受到了威胁。物理学家们在实验室中研究利用原子的特性,它们通过量子力学,而不是古典物理学来确定。由此,一种新型计算机的推出处于酝酿中。计划用这种新机型同样可以采取二进制形式储存或加工数据,如同用现在的计算机。但不同的

是，它不是通过或开或关的电子开关，通过充电或不充电的转换器，以及通过一块固定板上的强磁场，来形成二进制中的0和1，而是由分子的不同的量子态实现此项功能。在这种量子计算机中，天线电脉冲使分子由一种量子态转变为另一种。它比我们目前使用的计算机更为迅捷。美国的许多研究所都有课题组专攻量子计算机的研制。如果他们取得成功，对于密码学具有直接意义，因为大约在四年前，一位科学家在美国贝尔实验室发明一种程序，利用它在量子计算机上可以迅速将大数值分解为因子。

那么我们是否要为银行里的存款担心呢？将来会不会有人持伪造电子签字把我们洗劫一空呢？不过量子计算机并未问世，就算它出现了，那不仅分解大数值简单化了，而且我们可以通过更长的密钥数增加破译的难度。

对大数值进行因子分解以及突破这种 RSA 加密程序，将作为数学问题留存，人们只能以集体作业的大规模方式研究它，而不可能在静静的小屋中。所以即使面对窃贼，我们由 RSA 保护的财产就是在将来也会如同美国诺克斯城堡中的金子一样安全——但愿如此。

附录 A

自制密码机

我们在 153 页提到的伦敦记者罗伯特·马修斯，在 1989 年发表了一篇关于一种简单密码机的组装及使用说明。[1] 这种密码机由两张纸片组成，其上沿和下沿被粘合成一张纸片，并能在一个圆柱体上被对着弯曲。马修斯建议，可以利用装小型胶片的暗筒作为滚筒；我则选用了一只卷笔刀的套子(图 A.1)。两张纸片则见于图 A.2。

无论你用什么作滚筒，都必须将图 A.2 用复印机复制到一张纸上。根据滚筒的尺寸，你必须在复印时作相应的扩大或缩小。然后沿垂直线将这个长方形区域剪开，现在你面前有两个部分，其中一部分有 2 栏，另一部分 4 栏。如果你按合适的尺寸制造复印件，那将两张剪开的纸条放在滚筒上，并且做到完全贴合及能相对转动，这并不难。然后你用合成薄膜绝缘带把它们的末端粘合起来，左边那张是 2 栏的，右边是 4 栏的。左边上面是字母表(其中 i 和 j 不分，因而字母表上只有 25 个字母)，右边是数字，有一处还有一个指向左边的箭头。左边的纸条上，每个字母有一个数字对应。

---

[1] "一种用于周期或随机密钥加密的转筒装置"，《密码学》，1989 年 7 月，第 266 页。

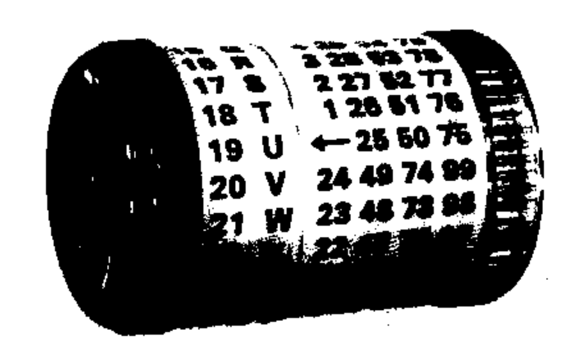


图 A.1:自制密码机。由图 A.2 得来的纸条绕在卷笔刀上。它们相对转动。文中解释了如何用它来加密。

接下来我们可以按照维吉尼亚方式,使用有限密钥词或按一次性密码本(见 166 页),采用任意长度的随机数字。

我们先从密钥词入手,简单地选用 HUND(狗)。借助左边纸条,我们可以制造出一个密钥数,它的各个组成部分 07 19 12 03,分别对应密钥词的 4 个字母。现在我们把 rose(玫瑰)作为明文词加密。为此我们旋转右边的纸带,使得有密钥数 07 的那一行同有第一个明文字母 r 的那一行对应起来。于是右边纸带上的箭头指示出第一个密文字母,即 Y。然后我们旋转第二个密钥数,19,对应上面第二个明文字母,o。箭头指向 H。如果我们如此进行,就可以从 rose 得出相应密文 YHEH。总的来说,加密规则是这样的:将明文字母和密钥数调至同一行,这样箭头指向密文字母。

0	A	*1*	*26*	*51*	*76*
1	B	←	*25*	*50*	*75*
2	C	*24*	*49*	*74*	*99*
3	D	*23*	*48*	*73*	*98*
4	E	*22*	*47*	*72*	*97*
5	F	*21*	*46*	*71*	*96*
6	G	*20*	*45*	*70*	*95*
7	H	*19*	*44*	*69*	*94*
8	I	*18*	*43*	*68*	*93*
9	K	*17*	*42*	*67*	*92*
10	L	*16*	*41*	*66*	*91*
11	M	*15*	*40*	*65*	*90*
12	N	*14*	*39*	*64*	*89*
13	O	*13*	*38*	*63*	*88*
14	P	*12*	*37*	*62*	*87*
15	Q	*11*	*36*	*61*	*86*
16	R	*10*	*35*	*60*	*85*
17	S	*9*	*34*	*59*	*84*
18	T	*8*	*33*	*58*	*83*
19	U	*7*	*32*	*57*	*82*
20	V	*6*	*31*	*56*	*81*
21	W	*5*	*30*	*55*	*80*
22	X	*4*	*29*	*54*	*79*
23	Y	*3*	*28*	*53*	*78*
24	Z	*2*	*27*	*52*	*77*

图 A.2：此处所示的数表可以在复印机上放大或缩小，使之完全符合圆柱体的尺寸，如图 A.1 所示。然后将得到的数表沿画出的线剪开。把两条纸带放到圆柱体上并粘到一起。然后必须能相对转动。

脱密相应进行。脱密者知道密钥，即数串 07　19　12　03，所能看到的是密文 YHEH。他将箭头旋转至指向第一个密文字母，即 Y，于是我们就得到了第一个密钥数，07，r。以此类推，由 YHEH 又推出 rose。脱密的普遍规则：旋转箭头至密文字母，再由密钥数得出明文字母。

如果所涉及的是一个任意长度的密钥词或密钥数，也无甚不同。假使我们再以《苏菲的世界》开头部分作为绦虫式密钥，如第七章所述，那我们必须借助左边纸带，把密钥字母派给明文。

附录 B

把我的电脑当作“恩尼格玛”机

汉堡大学的计算机学家玛丽安·卡索维科编写了一条能将她的计算机转化为“恩尼格玛”机的程序。你能从因特网上获取这条程序以供个人使用。为此，必须接通因特网。如果你有某个朋友上了网也行。你必须先将程序 enigma22.exe 装入电脑，然后键入

enigma22

接下来将出现许多新文件，其中有两个末尾带有.doc.文件 swissen.doc 告诉你“恩尼格玛”机是如何运作的，enigma.doc 则是“恩尼格玛”程序 senigma.exe 的使用说明。你必须仔细阅读这两个文件，然后就能着手行动了。输入

senigma

你眼前的屏幕上将构造出一个“恩尼格玛”机的示意图，电脑的键盘就是机器的键盘，屏幕上将有 26 个区间发亮，它们代表“恩尼格玛”机的小灯泡，你会在字母窗中看见轮子上的字母。这时，必须设制你的“恩尼格玛”机，为此输入符号/。如果你已忘记文件 enigma.doc 中的使用说明，它将把这一过程向你重新解释一遍。你可以选择三密钥轮或四密钥轮“恩尼

格玛"机,然后从8个可置换的密钥轮中挑出3个装入机器并确定密钥轮位置。如果你选择的是四密钥轮"恩尼格玛"机,可再装入一个希腊密钥轮(B,C为Beta密钥轮与Gamma密钥轮),以及配套的薄型互动轮。你可以选择缺口环位置与插塞连接,并把轮子调到基本位置。输入1,屏幕左边将有两个区间显示出你是如何设制"恩尼格玛"机的,这样,你就能够编写密码了。

输入明文,你将看到,右边的密钥轮是如何随着单个字母滚动,并不断带动中间的密钥轮一步步移动。与此同时,在屏幕下方的两行当中将出现明文与密文。你可以相信,在输入明文之后,你将会获得一份密文。如果在密钥轮相同起始位置下,输入这份密文,则又能得到明文。你也可以检验246页上所描写的四密钥轮式"恩尼格玛"机的特性:如果程序中标有字母B的希腊密钥轮Beta在窗口显示出字母A,并且这时已装入程序中标有字母B的互动轮,那么这台四密钥轮机的编密方式就与三密钥轮机相同,后者的轮子处在与前者3个活动密钥轮一样的起始位置。

附录 C

如何确定三个魔幻的密钥数

取两个素数，我们把它们叫作 p 和 q，在 249 页的加密例子中为数字 5 和 7，253 页的例子里 p = 48611，q = 1009。选好这两个数之后，把它们相乘就得出第一个幻数 N。在第一个例子中 N = 85，第二个中 N = 49048499。现在我们还要计算一个辅助数字，我想把它称为 z。如果将 p 和 q 都减去 1 并将结果相乘，就会得到这个数。在第一个例子中 z = (p – 1)(q – 1) = 64，第二个例子中 z = 48610 × 1008 = 489988880。数字 z 有助于我们确定 E 和 D 这两个密钥数。其中有个数字，比如说 E，较容易确定，它只需具有不能被 z 整除的特性就行。数字 z 能被 4 整除，因为 p 和 q 应该为奇数（没有人会产生这种想法，即用素数 2 作为二者之一，因为如果这样的话，秘密就会立即暴露出来，我们即将看到这一点）。如果 p 和 q 为奇数，那 p – 1 和 q – 1 为偶数，于是 z 能被 4 整除。从中已能得出结论，E 必须为奇数，否则它与 z 都能被 2 整除。

如果有谁想把这些弄得简单点，那么就直接选择一个比 z 小的素数，并通过除法检验它是否包含在 z 中。如果是，就尝试用另外一个素数，如果不是，那么他就可以用它作为 E。我们在第一个例子中选择 E = 5，第二个例子里 E = 61，这两个素数都不包含在相应的 z 当中。

现在我们已经有两个公开的密钥数 N 和 E。最重要的当然是第三个，即秘密的密钥数 D，我们还得为它下一番功夫呢。数字 D 必须具有以下特征：与 E 相乘后除以 z 必须余 1，即 $E\times D\equiv 1(\mathrm{mod}\ z)$，我先用简单点的例子 $z=64$ 来演示一下 D 的计算过程：

取出 z 和 E，用小的数除大的数并确定余数。在我们这个例子中 $z=12E+4$，余数为 4。接着我用余数 4 除 E：$E=1\times 4+1$，余数为 1。如果余数为 1，那么我的计算就完成了。如果我选择的 E 不能被 z 整除，那我迟早会得出余数 1。现在进行第二部分的计算：我从最后一个等式开始并将 1 写在左边：$1=E-1\times 4$，用前一个等式的余数代替 4，即 $1=E-(z+12E)$ 并整理为 $1=-z+13E$，我们的要求即 $E\times D$ 除以 z 的余数必须等于 1，就已满足了。现在我们转到余数上来，在两边都加上 $z=64$，于是就得到余数 $1\equiv 13E(\mathrm{mod}\ z)$。所以 $D=13$。

我们现在怎样才能把这个像变魔术般的计算过程总结成一条简单的规则，按照这条规则我们就能在其他例子中引进这个秘密数字 D？最好的制订这条规则的办法是把 z 叫作"第一余数"，E 叫做"第二余数"，这听起来有点儿难以理解，因为我根本就没有进行除法计算，为什么要把它们称为余数呢？但我们将看到，这样是制定规则的最好办法。我们已在上面用第二余数 E 除了第一余数 z 并得到第三余数 4。然后用第三余数 4 除第二余数 E 并得到第四余数 1。我们可以从中得出以下规则并将其作为食谱：

用第二余数除第一余数，以得到第三余数。然后用第三余数除第二余数以得到第四余数，以此类推。从第三个开始，每个余数都是通过将它前面第一个余数除它前面第二个余数来确定的，直到得到余数 1。接下来从最后一个等式开始，把

1写在左边，其他的全部写在右边，然后通过前面的等式代替所有出现的余数，直到最后1用第一和第二余数，即 z 和 E 表示。如果我们转到与 z 有关的余数上来，那么含有因数 z 的加数就会消失，于是 D 就是 E 的因数。

我想再通过 $z = 48998880$ 和 $E = 61$ 的例子将此过程再演示一遍。第一余数为 z，第二余数为 E，第一余数除以第二余数：$z = 803260E + 20$ 得到第三余数 20，第二余数除以第三余数 $E = 3 \times 20 + 1$ 得出第三余数为 1，我们完成了第一步。从后往前算：

$1 = 3 - 2 \times 20 = E - 3(z - 803260E) = -3z + 2409781E$，所以 $1 = -3z + 2409781E$ 或者 $1 \equiv 2409781 \pmod{z}$；从而得出秘密数字 $D = 2409781$。

通过这种方式我们可以确定一个神秘的三重数字，我没有证实是否真的能够利用一个这样确定的数字进行加密，即是否能通过第十二章中描写的方式，用 N 和 E 将每个明文数字制成一个密文数字，而且这个密文数字又能借助 N 和 D 重新变回明文数字。这需要一项数学证明，读者能在我列出的弗里德里希·L·鲍尔和阿尔布雷希特·博伊特尔斯帕赫尔的书中找到这一证明。

除了一点儿计算之外，确定秘密密钥数 D 并无其他难处。于是就可以下结论，认为格劳先生在得知公开的密钥数 N 和 E 之后就能发现秘密数字 D 吗？决不可能，因为我们在计算 z 时采用的不是 N 和 E，而是产生 N 的 p 和 q 这两个素数。我们是通过这两者减 1 之后相乘得到数字 z，而格劳先生却不知道这一点，因为这两个数字处于严格保密中。实际上，加密的秘密在于将数字 N 分解成两个素数。在 $N = 85$ 的例子中较容易分解——每个中学生都能看出 85 能被 5 整除；相

除之后，得出第二个素数，17。知道这两个素数后，他就能计算 z，并用我们刚才同样的方式从公开的数字 E 中确定出 D——加密方法就被破译了。我们要牢记：一旦隐藏在 N 中的两个素数被发现，密码就会破译。这对数字 85 来说比较容易，但是当 N = 49048499 时难度就更大了，而当数字超过 100 位时，在实际操作中根本不可能做到这一点。

还有一个值得提醒的地方：我已在此解释了在确定 p 和 q 以及 N 后，如何选择数字 E 并从中计算 D。相反，我也可以选择 D，然后计算 E。E 和 D 同等重要。我们在文中总是以 E 为公开的密钥而 D 为秘密的密钥数，这纯粹是随意的。我们也可以选择 D 为公开密钥数而 E 为秘密的密钥数。

附录 D

PGP,从因特网上取下的加密程序

……无需任何代价。你不必是电脑天才,也不需要什么特别精密的个人电脑,在我这台 1990 年的 386 上,这个程序运行得相当出色。我甚至还在放在地下室里无人可送的老式 IBM - 个人电脑 PS/2 - 30 上操作了这一程序呢。

在因特网上,人们可从多个地方获得 PGP 程序。我是从曼海姆大学的学生那里得到这个程序的。在万维网上的地址为:

http://www.uni - mannheim.de/studorg/gahg/PGP/

你将在那儿发现许多带有 pgp 标记的程序,紧接着还有许多符号,末尾是 zip。我从那儿将 pgp263ii.zip 复制到我的光盘上,而且还有一个熟人给我的程序 pgp262ii.zip。

附加符号 zip 表示这是一个压缩过的程序,你必须先把它扩展。为此还有一个叫做 pkunzip.exe 的小程序,这一程序可能已经存在于你的计算机中,或者你也可以通过熟人弄到它。把 pgp263i.zip 放入你在计算机中为 PGP 制作的图表里,图表的名字为 PGP。程序 pkunzip.exe 同样也必须存入这张表中,除非你把你的计算机设制成,无论在哪一张图表中工作,都能完全使用辅助程序。现在给出命令

pkunzip.pgp263i.zip

这时屏幕上会有所动静，出现一大串名字并且这些名字不断往上移，以让位给新出现的名字。从我的压缩过的程序中就产生出二十多个新文件，我们现在只应对其中的一个感兴趣：pgp.exe，它是用于PGP（绝对隐私）的程序。

你能在克劳斯·舍恩莱伯和菲利普·齐默尔曼随书附上的光盘中找到PGP的程序设制。西姆森·加芬克尔的书带有一张3.5寸的软盘，其中包括用于驱动系统DOS和UNIX的两个程序设制。

PGP的建立

你可以在文件pgpdoc1.tet和pgpdoc2.tet中找到一份英文的使用说明。我在此为那些只想了解基本原则的读者描述几种该程序的简单使用方法。

如同每个RSA程序一样，PGP也需要3个神秘的密钥数：适用于每个使用者的N，公开的E和秘密的D。然后，程序才能用于编码和脱密。当然，你不必自己按照附录C的方法来确定密钥数，程序会替你解决这一问题。为此你输入

pgp - kg

连接号之前必须有一个空格。接下来会出现一大篇解释，你暂时不用去理睬它，在此之后程序会向你提供一个选择。你可以选择短的、较长的或十分长的密钥数。① 加密方法也就与之相应难，较难或非常难破译。你选取一个保密程度。现在你需要用它来输入一个标志，User - ID，通过它电脑可以将

---

① 在我的老式"地下室电脑"上，程序首先要求我在主图表中再设制一张名字为temp的小图表，也许是需要用它来储存中间数据。

你重新辨认出来。输入你姓名的缩写，施瓦茨太太只要选择"schwarz"就行了。User - ID 还不是什么秘密的东西，它直到现在才出现，因为电脑要求你确定一个密码，它是一个不能让别人知道的秘密符号。输入一个无人能够猜到的字母和数字的组合，如 xyzoed78。不过你必须记住这个密码。为了检验，电脑会让你再次输入同一密码。

现在谈谈这3个神秘的密钥。你还需要一个公开的E和一个秘密的D。为此，计算机会让你输入一段较长的文章，通过打字的节奏来确定E和相应的D。例如，开始输入你在中学时代学过的一首诗，一段时间后，计算机会说现在够了。它开始计算，屏幕上会出现一行或多行点号和星号。于是程序就完成了工作，你的两个密钥数都已被确定。那个公开的密钥数在一个名为 pubring.pgp 的文件中，为了读出这一文件，必须键入

pgp - kv

于是你将在屏幕上发现一连串字母，如

pub 512/59184C2D1996/09/22 schwarz

这个带有 512/59184C2D 标记的公开密钥，产生于1996年9月22日，属于 schwarz。

然而，为了能与你周围的人交流加密的信息，你还有更多工作要做：将你的公开密钥告诉别人并且知道别人尽可能多的密钥。为此可采用一张清单，把你的文件 pubring.pgp 复制在一张磁盘上，并给它取另外一个名字，比如 liste.pgp。你必须与用同样的PGP程序工作的通信伙伴交流这一文件。

但是我们暂时只为一个使用者设制 PGP。至于几个人在他们的计算机上通过刚才描述的方式装入 PGP 之后，怎样利

用 PGP 来交流信息，我将在我办公室里的两台电脑上进行说明。

我在每台电脑上分别装上一个 PGP 程序，在其中一台上，我扮演施瓦茨女士的角色，输入"schwarz"作为 User - ID，并为她选择一个密码(为了简便起见采用 sOsOsOsO)。在另一台电脑上我以魏斯先生的身份输入相应的东西：User - ID 为"weiss"，密码为 wOwOwOwO。我给这两者都选择相同的保密程度。当我在两台机器上按要求输入一篇较长的文章之后，程序就为使用者 weiss 和 schwarz 确立了各自的密钥 E 和 D，这些数字分别位于图表 pubring.pgp 中。现在我只需要告诉每台电脑对方的公开密钥就行了。每个人暂时只在他的 pubring.pgp 文件里有自己的公开密钥，而这份清单却存于盘中 liste.pgp 文件名下。于是魏斯和施瓦茨交换各自的磁盘并将文件 liste.pgp 复制到各自的图表 PGP 中，然后，每个人都键人

pgp - ka liste.pgp pubring.pgp

这时，程序在文件 liste.pgp 中寻找程序中还没有的公开密钥。魏斯先生的程序找到了施瓦茨女士的公开密钥并把它加到自己的文件 pubring.pgp 中，施瓦茨的程序也采取相应的做法。现在每个人都获得了对方的公开密钥。

用 PGP 加密

魏斯先生想通过加密的方式将信息"morgen um acht am bahnhof"(明天 8 点火车站见)寄给施瓦茨女士。他在电脑上用一个文件处理程序，最好是 DOS 版本输入这条信息，并给该文件命名，比方叫 brief1.txt。然后把它存入图表 PGP 中，接

着输入

pgp – e brief1 .txt schwarz

schwarz 这个词告诉电脑，它该利用施瓦茨女士的公开密钥。图表中出现了一封带有名字 brief1 .pgp 的密码信，魏斯先生将其复制到一张磁盘上并把它寄给了施瓦茨女士。

用 PGP 脱密

她把这张磁盘塞入她的电脑并将这条加密信息复制到图表 PGP 中，接着输入

pgp brief1 .pgp

因为要利用施瓦茨女士的秘密密钥来脱密，程序必须确定电脑旁坐的是否真是施瓦茨女士。它向她询问密码，她将其输入，于是 brief1 .txt 的明文又出现了。

用 PGP 签名

魏斯先生寄给迈尔霍费尔博士的信需要一个电子签名。用 PGP 的方法如下：魏斯先生用一个文件版本输入一则信息，给它命名为 nachr.txt 并把它转移到图表 PGP 中。然后键人

pgp – s nachr.txt weiss

我们知道，“weiss”是他的 User – ID。因为必须利用他的秘密密钥来进行电子签名(见 292 页)，程序会向他询问密码。他将密码输入后，会出现一个利用魏斯先生的秘密密钥加密的文件 nachr . pgp。

如果收信人在图表 pubring.pgp 中已有魏斯先生的公开密钥，电脑就会告诉他，这份文件只可能来自于魏斯先生，因为只有通过魏斯先生的公开密钥才能进行脱密。另外，它会产生一个名叫 nachr.pgp 的文件，它包括了明文，而且迈尔霍费尔先生通过一个文件版本能在他的电脑上将其读出。

[General Information]
书名=密码传奇
作者=(德)鲁道夫·基彭哈恩著
页数=314
SS号=0
出版日期=